



Trinity College Dublin

Coláiste na Tríonóide, Baile Átha Cliath

The University of Dublin

School of Computer Science and Statistics

DNS Abuse Transparency

Abdelaziz Abushark

Supervisor: Dr. Stephen Farrell

April 4, 2024

A dissertation submitted in partial fulfilment
of the requirements for the degree of
Computer Science and Business

Declaration

I hereby declare that this dissertation is entirely my own work and that it has not been submitted as an exercise for a degree at this or any other university.

I have read and I understand the plagiarism provisions in the General Regulations of the University Calendar for the current year, found at <http://www.tcd.ie/calendar>.

I have completed the Online Tutorial on avoiding plagiarism 'Ready Steady Write', located at <http://tcd-ie.libguides.com/plagiarism/ready-steady-write>.

I consent / do not consent to the examiner retaining a copy of the thesis beyond the examining period, should they so wish (EU GDPR May 2018).

I agree that this thesis will not be publicly available, but will be available to TCD staff and students in the University's open access institutional repository on the Trinity domain only, subject to Irish Copyright Legislation and Trinity College Library conditions of use and acknowledgement. **Please consult with your supervisor on this last item before agreeing, and delete if you do not consent**

Signed: _____

Date: _____

Abstract

This research project explores the vital subject of DNS (Domain Name System) abuse, which is widespread and jeopardises the reliability and security of the Internet. The integrity of DNS operations has become critical due to the growing reliance on the internet for both personal and professional activity. To promote a safer online environment, this project aims to increase transparency within the DNS ecosystem by examining the forms, effects and current mitigating techniques of DNS abuse. DNS abuse poses serious threats to internet security and includes phishing, confusable domains (typosquatting), domain hijacking, botnets, quick flux hosting, and domain generation algorithms (DGA). Every type of abuse puts users at risk by making identity theft, money loss, data breaches, and system intrusions easier, as well as by undermining confidence in online services. The research project emphasises how urgent it is to address these problems because new technologies like IoT, cloud computing, and AI have the potential to make them worse.

The methodology used in this study included a thorough examination of the DNS ecosystem, vulnerability identification, and an assessment of the mitigation initiatives that are currently being undertaken by important parties, such as registries and registrars. Surveying DNS infrastructure providers and stakeholders was a major part of the investigation to determine the existing level of transparency in the mitigation of DNS abuse. This involved assessing the usefulness of transparency reports and how well they work to stop DNS abuse. Key findings point to a serious weakness in DNS abuse mitigation initiatives' openness. Although several organisations have taken positive steps towards transparency, there is still a lack of standardisation and fragmentation in the industry as a whole. The report makes a number of suggestions to improve openness, such as creating uniform reporting guidelines, encouraging greater cooperation between DNS stakeholders, and implementing best practices to deal with DNS abuse in an open and transparent manner.

This research project adds to the current conversation on DNS abuse by providing a practical reform plan and a detailed grasp of its complexities. It establishes the foundation for more successful mitigation of DNS abuse by promoting greater transparency, which ultimately results in a more secure and reliable Internet.

Lay Abstract

The goal of this project is to address DNS abuse to make the Internet safer. If you think of the Internet as a giant library, DNS is the index that lets you locate the specific book you are looking for. However, some people manipulate this index to point you to the incorrect book, one that could endanger you by installing malicious software on your computer, stealing your personal information, or stealing money without your knowledge. We refer to this type of deceit as DNS abuse, and it is a serious issue since it can cause people to lose faith in the internet. In this study, we examine how malicious actors use DNS to cause harm, how it affects regular internet users like you and me, and the measures taken to prevent them. We took particular note of the transparency and candour with which the Internet's operators handled these issues. We can all trust the Internet better if they are transparent about how they solve these problems.

To gain an understanding of this, we reviewed publications on countermeasures against DNS abuse and spoke with numerous individuals involved in the Internet's index system. We found that there is still a great deal of room for improvement, despite the fact that some people are making an effort to be more transparent about how they are solving the issue. There is no standard approach to solving or discussing the issue, and nobody is in agreement. Our findings imply that, in order for everyone to collaborate more successfully, we need to improve the system. To ensure that everyone is aware of the steps being taken to protect the internet, we should all be able to deal with DNS abuse in a uniform manner and have a conversation about it. Those who maintain the index system for the Internet may make it feel safer for all of us to use it by being more transparent.

This project clarifies the causes, consequences, and significance of communicating openly and clearly about mitigating DNS abuse. We want to contribute to the development of a safe and reliable online environment for all users by offering suggestions on how to improve.

Acknowledgements

In the name of God, the most Gracious, the most Merciful.

First, I would like to thank God. Everything I do is only done with his permission. I sincerely thank everyone who helped me along the way with this thesis. First, I express my sincere gratitude to Dr. Stephen Farrell, my supervisor, whose knowledge, compassion, and tolerance greatly enhanced my graduate experience. From the beginning to the end of my inquiry, your advice was very helpful.

I also would like to express my gratitude to the study participants who enthusiastically engaged with my work and offered valuable insights into the dynamics of DNS abuse.

I must express my sincere gratitude to my family for their unwavering support and unceasing encouragement during my years of education, as well as during the process of conducting research and composing this project. Without them, this achievement would not have been feasible. I am grateful to my parents for their guidance and experience.

Finally, I would like to thank Trinity College Dublin and my lecturers for giving me opportunities over the past four years. I am appreciative of what they have offered.

Contents

1	Introduction	1
1.1	Brief Context for the Problem	1
1.2	Motivation	2
1.3	Research Question/Project & Personal objective	3
1.3.1	Research Question	3
1.3.2	Project Objectives	4
1.4	Scope	5
1.5	Outline of the Project Work	5
1.6	Outline of the report	6
2	Background	8
2.1	Understanding DNS & Its Vulnerabilities	8
2.2	Strategies & Collaborations in Addressing DNS Abuse	9
2.3	Different Forms of DNS Abuse	10
2.3.1	Phishing	10
2.3.2	Confusable Domains (Typosquatting)	10
2.3.3	Domain Hijacking	10
2.3.4	Botnets	11
2.3.5	Fast Flux Hosting	11
2.3.6	Domain Generation Algorithms (DGA)	11
2.4	How DNS Abuse Harms Users	12
2.4.1	Identity Theft	12
2.4.2	Financial Loss	12
2.4.3	Data Breach	12
2.4.4	System Compromise	12
2.5	Future Dangers of DNS Abuse	13
2.5.1	Increased Sophistication	13
2.5.2	IoT Vulnerabilities	13
2.5.3	Infrastructure Attacks	13

2.5.4	Deepfakes & AI	13
2.5.5	Cloud Computing Vulnerabilities	13
2.5.6	Mobile Device Exploitation	14
2.5.7	Cryptocurrency & Blockchain Exploitation	14
2.5.8	Political and Information Warfare	14
2.5.9	Exploiting Emerging Technologies	14
2.5.10	Supply Chain Attacks	14
2.6	Foundational Mitigation Strategies & Best Practices	15
2.7	Summary & Synthesis	17
3	State of the Art	20
3.1	Current Strategies and Their Effectiveness in Relation to DNS Abuse	20
3.1.1	Transparency in DNS Abuse Mitigation & DNS Relevance	20
3.1.2	Effectiveness of Current DNS Abuse Mitigation Strategies	29
3.2	Emerging Trends in DNS Abuse	29
3.2.1	Evolving New Forms of DNS Abuse	30
3.2.2	Predictive Measures & Their Transparency	30
3.3	Technological Advancements	33
3.3.1	Role of AI & ML	33
3.4	Case Studies and Real-World Applications	34
3.5	Challenges & Future Directions	39
3.5.1	Identification of Current Challenges	39
3.5.2	Discussion on Future Research Directions and Technologies	40
3.6	Summary of Findings	40
4	Research Methodology	41
4.1	Questionnaire Design and Distribution	41
4.2	Stakeholder Responses	42
4.3	Types of DNS Abuse Encountered	43
4.4	Challenges in Mitigation and Mitigation Strategies	44
4.5	Transparency in DNS Abuse Mitigation	44
4.6	Impact on Relationships within the DNS Ecosystem	45
4.7	Analysis and Data	46
5	Implementation	49
5.1	System Overview	49
5.2	Integration	50
5.2.1	Backend Implementation	50
5.2.2	Frontend Implementation	51
5.3	Tools & Technologies	53

5.4	Visualisations	53
5.4.1	Input & Interaction	54
5.4.2	Interactive Features	54
5.4.3	Results Display	55
5.4.4	Navigating Results	56
5.5	Challenges & Solutions	56
5.6	Testing & Validation	57
6	Evaluation & Discussion	58
6.1	Confusable Domains	58
6.1.1	Identification & Examples of Targeted Domains	58
6.1.2	Real-life examples	59
6.1.3	Homograph attacks	59
6.1.4	Real-life Mitigations	60
6.1.5	Techniques for Mitigating Confusable Domains	61
6.1.6	Transparency in Mitigation Efforts	62
6.1.7	Analysis : Feasibility & Practical Challenges	64
6.2	Phishing	65
6.2.1	Real-life examples	65
6.2.2	Real-life Mitigations	65
6.2.3	Techniques for Mitigating Phishing	66
6.2.4	Transparency in Mitigation Efforts	67
6.2.5	Analysis : Feasibility & Practical Challenges	69
6.3	Collaboration Among Registrars, Registries, and DNS Collaborators	70
6.4	Benefits of Transparency	72
6.5	Drawbacks and Security Concerns	73
6.6	Limitations of Research Conducted on DNS Abuse Transparency	73
6.7	How well did the project meet the objectives?	75
6.7.1	Objective Fulfilment	75
6.7.2	Impact on Understanding DNS Abuse	75
6.7.3	Stakeholder Engagement	76
6.7.4	Practical Implications	76
6.7.5	Suggestions for Improvement	76
6.7.6	Future Vision	76
7	Conclusion	77
7.1	Brief Review	77
7.2	Main Results	77
7.2.1	Related back to Project Objectives:	77

7.2.2	Summary of Proposals:	77
7.2.3	Assessment of Contribution :	78
7.3	Future Work	78
7.3.1	Further Research Directions:	78
7.3.2	Practical Next Steps for Developing Transparency Best Practices:	79
7.3.3	Enhanced Transparency Practices for DNS Abuse Mitigation:	79
7.3.4	Future Directions in DNS Abuse Mitigation:	80
7.3.5	Contributions to Future Transparency Practices:	81
7.4	Reflection	81
7.4.1	Personal Learning:	81
7.4.2	Evaluation of Research Process:	81
7.4.3	Perspective on Research Findings and Contributions:	81
A1	Appendix	83
A1.1	Appendix numbering	83

List of Figures

1.1	How DNS works. Adapted from ?.	1
1.2	increase in DNS abuse incidents over time. Adapted from ?.	3
1.3	DNS ecosystem.	5
2.1	Different Forms of DNS Abuse.	11
2.2	How DNS Abuse Harms Users.	12
2.3	Future Dangers of DNS Abuse.	15
2.4	Mitigation Strategie.	17
3.1	DNS Ecosystem Contractually Related to ICANN (image courtesy of Verisign and originally published in SSAC 115 adapted from ?)	32
3.2	DNS tunneling communication between the attacker's command and control (C2) infrastructure and the victim's network.	35
3.3	SUNBURST backdoor's utilization of DGAs and its associated components.	35
3.4	The usage of Fast Flux techniques by the Smoke Loader malware family for dynamic C2 domain communications.	36
3.5	The usage of Fast Flux techniques by the Smoke Loader malware family for dynamic C2 domain communications.	36
3.6	Development trends in the majority of COVID-19-related phishing content hosting sites during the period from January 2020 to February 2021. Adapted from ?.	37
3.7	Top spoofed websites in COVID-themed phishing attacks (global), where the percentage in each column is the percentage of phishing volume per site and category. Adapted from ?.	38
3.8	Statistic of lifespan distribution of COVID-19-related phishing content hosting sites when the sites are reported. Adapted from ?.	38
5.1	Domain Legitimacy Checker	50
5.2	Domain Legitimacy Checker System Interaction Workflow	51
5.3	Domain Legitimacy Checker	52
5.4	The main interface of the Domain Legitimacy Checker	53

5.5	The domain input box where users begin their interaction with the Domain Legitimacy Checker.	54
5.6	The 'Analyze' button, poised for user action after domain entry.	54
5.7	Server log entries capturing real-time HTTP requests and responses	55
5.8	visual indicators showing the legitimacy status of analysed domains.	55
5.9	The 'Check Another Domain' button	56
6.1	confusables registered for popular domains, adapted from ?.	60

List of Tables

2.1	Mitigation strategies against DNS abuse and its impact on users.	19
4.1	Varied Definitions and Understandings of DNS Abuse	46
4.2	Types of DNS Abuse Encountered	46
4.3	Challenges in Mitigating DNS Abuse	47
4.4	Mitigation Strategies Employed	47
4.5	Transparency in DNS Abuse Mitigation	47
4.6	Impact on Relationships within the DNS Ecosystem	47

1 Introduction

1.1 Brief Context for the Problem

The Domain Name System (DNS), which turns domain names into IP addresses, is an element in the large and complex network of digital communications. This system has an impact on each user's everyday digital interactions, in addition to ensuring that the internet runs smoothly. Unfortunately, this system is not resistant to abuse. Malicious actors use DNS domains for a variety of illegal activities, such as sending malware, phishing websites, and controlling botnets[?]. These actions compromise the reliability and security of the Internet by posing serious risks to cybersecurity and user trust[?]. Addressing this issue requires a robust response from DNS infrastructure providers, including registrars and registries, who play a pivotal role in managing abuse complaints. Registries are organisations that manage top-level domains (TLDs) such as ".com" and ".net", and registrars are like a dealership for domain names. These entities have the authority to deactivate or deny the registration of DNS names if abuse is proven. Proactive measures are also considered, such as the prevention of registrations that could facilitate "typosquatting," and theoretically the regulation of permissible domain names to censor registration or renewal based on content. The effectiveness of these interventions could be significantly improved by adopting a transparent approach to the measures implemented and the rationale behind such decisions. Although the publication of transparency reports can illuminate these practices, their issuance is rarely observed in the current landscape.

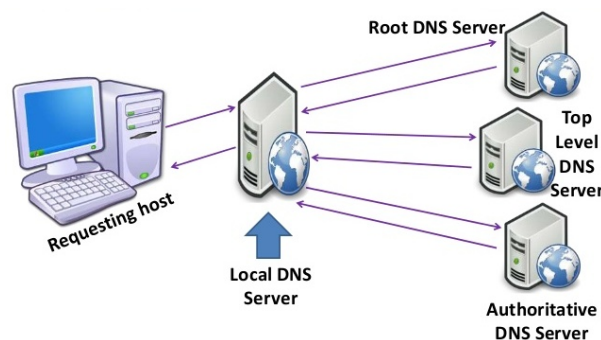


Figure 1.1: How DNS works. Adapted from [?].

The abuse of DNS extends beyond simple inconvenience; it is a serious flaw in the Internet's architecture that might have a big impact on people's privacy, business, and national security. Abuse techniques are numerous and constantly changing; they include confusable domains, which is the practice of creating malicious domains that imitate real ones, phishing, etc.?. All of these strategies can have disastrous outcomes, ranging from the theft of private information to the shutdown of important internet services. DNS security and mitigation of DNS abuse are important due to their central role in Internet operations. To counter these dangers, constant monitoring and proactive steps are needed. This includes communication between numerous parties, such as hosting companies, domain registrars, registers, researchers, and law enforcement, in addition to technology solutions ?.

1.2 Motivation

The Domain Name System (DNS) is a vital element of web activity in the age of technology, but malicious actors are increasingly interested in the system. The abuse of DNS for illegal activities such as confusable domains and phishing has raised questions about the integrity and security of the Internet. The severity and frequency of these concerns are highlighted in recent studies, such as the "Study on Domain Name System (DNS) Abuse: Technical Report" by Bayer et al. ?, highlighting the importance of more monitoring and mitigation tactics. Not only have significant cases of DNS abuse endangered user security, but they have also damaged the general trust in the digital economy. Users' trust in online services declines as they become more aware of these hazards, necessitating the implementation of mitigation measures to regain confidence and guarantee a secure online experience. According to Hesselman et al. ?, the idea of a "responsible Internet" aims to increase confidence and sovereignty by improving network-level transparency and accountability. Furthermore, Mathew and Cheshire's ? study "Trust and Community in the Practice of Network Security" dives into the significance of trust connections and communities in cybersecurity, demonstrating the negative effects of DNS abuse on user trust.

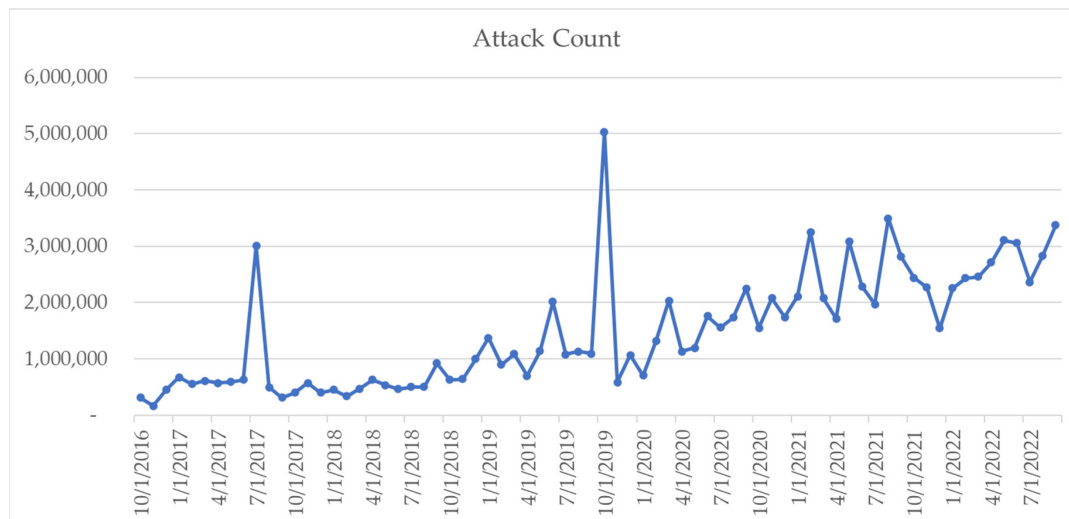


Figure 1.2: increase in DNS abuse incidents over time. Adapted from ?.

Organisations are leading the way in this issue, especially DNS infrastructure providers such as registrars and registries. However, their policies and activities tend to not be sufficiently clear. The continuous lack of confidence is made worse by the unclear way in which DNS abuse allegations are handled and the actions that follow. The importance of protecting the Internet and its reliability is recognised in relation to this issue ?. These difficulties are compounded by the average user's short attention span and diminished ability to comprehend information, as demonstrated by cognitive psychology studies like Medvedskaya's ? investigation of adult Internet users' attention spans. According to this research, consuming digital media may have a detrimental effect on one's capacity for sustained concentration, which would make grasping complicated topics even more difficult. Furthermore, there are ethical and legal consequences to DNS abuse and how to mitigate it in addition to the technical ones. The goal of this project is to close this gap by investigating ways to improve the transparency of DNS abuse mitigation. This study aims to shine light on the present efforts and highlight the obstacles to greater transparency by assessing the current landscape of transparency reports and practices among DNS infrastructure providers. The ultimate objective is to provide a contribution to a system that promotes and enables more efficient and approachable transparency in the mitigation of DNS abuse.

1.3 Research Question/Project & Personal objective

1.3.1 Research Question

The primary research question for this project is: "What strategies and practices are registries, registrars, and other parties involved in DNS infrastructure utilising to mitigate DNS abuse, and how do the transparency reports available from these entities characterise

and reflect their efforts? Furthermore, how could these practices and reports inform the development of best-practices for transparency in handling DNS abuse complaints?". This question seeks to uncover the mechanisms, policies, and practices in place to mitigate DNS abuse and to what extent these efforts are transparent to the public and stakeholders.

1.3.2 Project Objectives

Assess handling of abuse complaints

- Investigate the procedures and policies that DNS infrastructure providers have in place to handle abuse complaints.
- Document the types of DNS abuses that are most frequently reported and the response strategies used.

Assess Transparency Levels:

- Analyse the current state of transparency in the actions taken by providers against DNS abuse.
- Identify what information is made public, how it is communicated, and the frequency of disclosure.

Benchmark against Best Practices:

- Compare the findings with best practices in the industry to identify areas of strength and opportunities for improvement.
- Highlight exemplary cases of transparency and effective abuse mitigation.

Develop recommendations :

- Propose actionable recommendations for DNS infrastructure providers to improve their abuse handling and transparency.
- Suggest policy changes or initiatives that could standardise and improve practices in the industry.
- Feed into future work on ways in which best practices for transparency could be developed.

Contribute to stakeholder understanding:

- Provide insights that help stakeholders, including users, policymakers, and other providers, understand the landscape of DNS abuse handling and transparency.
- Offer a foundation for further research and discussion on improving DNS security and trust.

1.4 Scope

The Scope of this project is to perform a detailed examination of the transparency measures taken by registrars and registries to mitigate DNS abuse and to survey registries, registrars and others involved in mitigating DNS abuse to collect and characterise the transparency reports currently available. Examining the different types of data released, quantity and quality are all part of this process, as well as examining current transparency reports to inform future work on ways in which best practices for transparency could be developed. To obtain opinions and insights on current procedures and difficulties, the project will interact with a variety of players in the DNS ecosystem, such as registries, registrars, and policy makers. As part of the research, a set of criteria will also be developed to assess how transparency affects the views of Internet users about trust and safety. It will, however, not include the development of brand-new transparency tools or systems; rather, it will concentrate on examining current procedures and making recommendations for improvements. The main goal of the research is to understand and enhance transparency and its impacts.

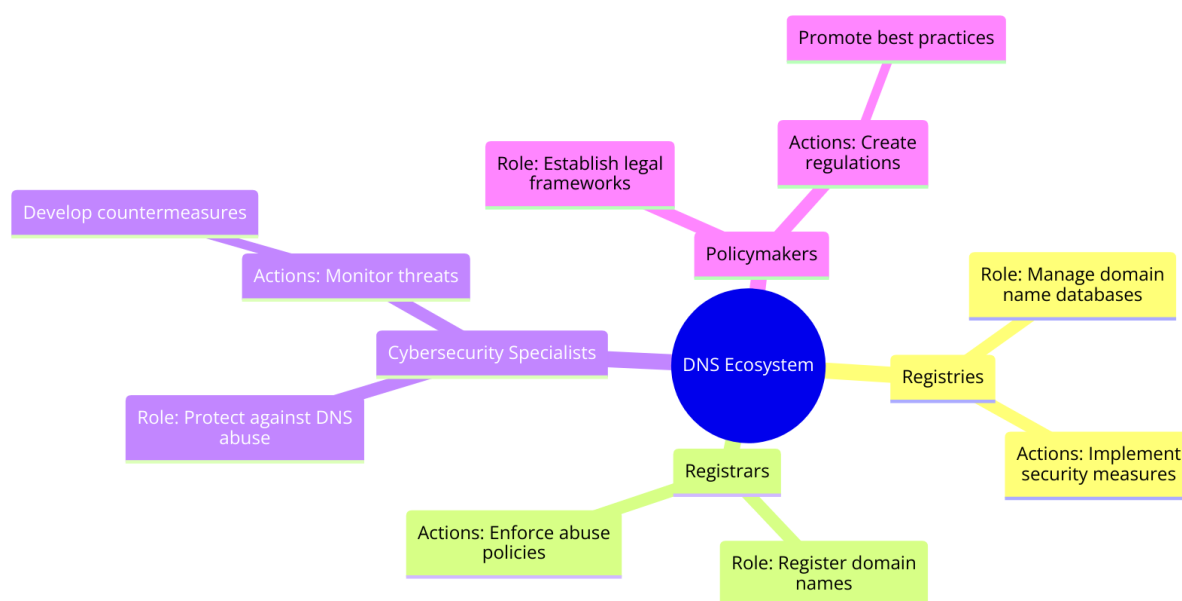


Figure 1.3: DNS ecosystem.

1.5 Outline of the Project Work

The goal of this project, "DNS Abuse Transparency," is to better understand and increase the transparency of the efforts of the registrars and registries to mitigate DNS abuse. Research will first examine the different aspects of DNS abuse, such as popular forms like phishing, confusable domains, etc. and their broader consequences. The project's later phases will be initiated by this fundamental understanding.

Data gathering will be based on a carefully planned questionnaire that will be distributed to a variety of DNS infrastructure providers and stakeholders throughout the world. The questionnaire attempts to shed light on current practices, the scope and efficacy of transparency measures, and the difficulties encountered in mitigating DNS abuse. At the same time, an examination of the transparency reports currently available from different sources will provide information on the transparency landscape, including the frequency, scope, and accessibility of these reports for users.

Critical evaluation of the handling of DNS abuse reports forms the core of the project. This involves looking at any proactive security measures that may be in place as well as the procedures for dealing with and preventing abusive domain registrations. After that, the research will change its focus to assessing how transparency affects user trust, provider reputation, and the general effectiveness of abuse mitigation techniques.

The project will discover and clarify best practices for transparency in the mitigation of DNS abuse, based on the data and insights obtained. The careful balance between security, privacy, and transparency will be taken into account by these best practices. The project will produce a series of practical suggestions for DNS infrastructure providers based on these findings, with the goal of improving transparency and, consequently, security and confidence in the digital ecosystem.

The project is designed to take place in a sequence of phases, each characterised by distinct deliverables. A comprehensive timeline will guide the progress, guaranteeing an organised and exhaustive study of the subject. Upon completion, this project will have contributed a collection of recommendations and considerations for future study and policy creation in this area of Internet governance, in addition to offering a comprehensive understanding of the current state of DNS abuse transparency.

1.6 Outline of the report

This report offers a comprehensive account of the steps performed, decisions made, and research carried out during the project's development. The format of the report is as follows:

Chapter 2 - Background

This chapter examines the foundations of DNS , along with its significance, weaknesses, and several types of abuse. Observe the tactics and alliances used to combat DNS abuse, including the work of ICANN and the DNS Abuse Institute. The topic of DNS abuse is discussed along with its effects on users and potential risks in the future, with a focus on mitigation techniques and recommended practices.

Chapter 3 - State of the art

This chapter critically analyses current strategies for DNS abuse mitigation and evaluates their effectiveness. Explores the complex relationship that exists between international governments and DNS, highlighting efforts to openness made by companies such as Google and Cloudflare. In addition to stressing the difficulties in striking a balance between user privacy and compliance requirements, the chapter emphasises the importance of DNS in internet governance. It investigates how various tactics are used and their effects on the larger online ecosystem through critical analysis.

Chapter 4 - Research methodology

This chapter describes techniques to investigate DNS abuse and transparency from the infrastructure provider. The author goes on how the questionnaires were made, how the responses from stakeholders were analysed, and what kinds of DNS abuse were found. This chapter describes the methodology used to collect and examine data to understand DNS abuse reporting procedures and transparency policies.

Chapter 5 - Implementation

This chapter involves the practical application, which involves findings from the project, especially the integration of the system, the back-end, the front-end implementations, and the technologies that comprise it. It includes how DNS data on abuse are visualised and the solution to the challenges during the implementation of the system. This part also includes testing and validation to ensure the success of the project.

Chapter 6 - Evaluation & Discussion

This chapter assesses how well the project addresses DNS abuse mitigation and improves transparency. It evaluates the advantages of transparency in DNS abuse mitigation as well as the security risks involved. The chapter also addresses the research limits and the degree to which the project's goals were achieved.

Chapter 7 - Conclusion

This chapter summarises the project's results and recommendations to enhancing DNS abuse mitigation transparency. Consider the difficulties faced, the importance of continuous attempts to improve DNS security, and the possibilities for further study in this field. In conclusion, the importance of cooperation and transparency is emphasised in the fight against DNS abuse.

2 Background

This chapter will explore the fundamental information relevant to this project, with an emphasis on the world of DNS abuse and transparency. It will include a detailed investigation of the domain name system (DNS), its function in the online community, and the variety of abuses it faces, the history of widely used policies and organisations aimed at mitigating DNS abuse, including a thorough examination of the DNS Abuse Institute and its achievements. A 'competition landscape' providing an examination of current market choices, from automated solutions to human tactics, will be provided as we navigate through the current methodology and technology deployed to mitigate DNS abuse. The reader will obtain a detailed understanding of the current situation of DNS abuse and the need for a more open, strong, and proactive strategy by analysing these various techniques and appreciating their strengths and weaknesses. This chapter emphasises the importance of the suggested solution in an era where digital authenticity is required, not only by providing information, but also by laying the groundwork for its presentation as a better and essential progression in the battle against DNS abuse.

2.1 Understanding DNS & Its Vulnerabilities

The Domain Name System (DNS) is a significant part of the Internet infrastructure, serving as the key to converting computer-understandable IP addresses into human-friendly domain names. Although the DNS plays a vital role in maintaining ongoing online activities, privacy and security problems still arise. The ScienceDirect paper "Domain Name System Security and Privacy: A Contemporary Survey" provides a detailed analysis of these concerns that highlights the fundamental importance of DNS while illuminating the weaknesses that malicious actors may take advantage of. There are a variety of security threats, ranging from DNS infrastructure targeting distributed denial-of-service (DDoS) assaults to cache poisoning and hijacking. Each of these attacks has the potential to do significant harm, including interruptions in service and the promotion of theft and spying. Due to the standard DNS design's lack of encryption, users' query data is vulnerable to abuse and eavesdropping, raising serious privacy problems. However, weaknesses do not mark the end of the story. In the same survey, new approaches are examined to improve DNS security and

privacy. The use of DNSSEC (DNS Security Extensions), which authenticates DNS data and guarantees its integrity while repelling some types of attack, is an example of these advances in security measures. In addition, privacy-enhancing technologies are being used to encrypt DNS queries, preventing eavesdropping and manipulation, such as DNS over HTTPS (DoH) and DNS over TLS (DoT). The environment of DNS threats and defences is always changing in sync with the Internet. For systems to be robust and resilient, it is essential to understand these weaknesses and the continuous efforts being made to mitigate them. In this section, we provide an in-depth discussion of DNS vulnerability details, the effects of these safety concerns, and creative solutions that aim to bring in a new era of DNS security and privacy.

In a usual DNS lookup, three types of queries come into play to streamline the process and minimise the data journey. The first type is a recursive query, where the DNS client expects a direct answer or an error if the record cannot be found from the DNS server. Then there is an iterative query, which means if the server doesn't have the answer, it points the client to another server that might know, and the client keeps asking down the line until it gets an answer or hits a dead end. Lastly, a non-recursive query happens when the DNS server already knows the answer either because it is directly responsible for that piece of information or it has it saved from earlier inquiries. This method helps to reduce unnecessary internet traffic and reduce the load on the servers involved.

2.2 Strategies & Collaborations in Addressing DNS Abuse

The DNS Abuse Institute, which will focus on DNS abuse to help increase safety and security through the domain name system, will be catered on these efforts to address DNS abuse with a comprehensive approach throughout the internet infrastructure. It helps the Internet community identify, report and mitigate DNS abuse in its mission to make the online environment more secure. Efforts by the institute, such as Compass Dashboards, provide vital data to registries and registrars that will enable proper decisions on combating DNS abuse. They show the commitment to transparency and education by issuing publications such as the "DNSAI 2022 Annual Report" or "DNSAI Bulletin 2023 04; Account Takeovers," which provide information on DNS abuse and how recommended mitigation practices ?. Another such global strategy against DNS abuse has been contributed by the Internet Corporation for Assigned Names and Numbers (ICANN)? in collaboration with the entire DNS community, ICANN supports a synchronised method in the development of policies and standards on how to mitigate DNS abuse while ensuring the openness of the Internet. These participatory pillars hint at concerted efforts through policy development, technological developments, and stakeholder engagement as a central

component in this collective approach to combating DNS abuse ?.

2.3 Different Forms of DNS Abuse

DNS abuse takes many forms, each with its procedures and effects on users and the Internet as a whole. It is essential to understand these various pieces of evidence to create responses and regulations that work. This section will examine the comprehensive analysis of DNS abuse presented, describing the description, mechanism, and impact of each kind ?.

2.3.1 Phishing

- **Description:** Phishing is a technique aimed at deceiving individuals by creating website addresses that mimic those of companies, to trick users into revealing sensitive information such as login credentials, credit card numbers, or personal identification information ?.
- **Mechanism:** This deception often occurs through emails or messaging services that direct users to websites similar to authentic ones ?.
- **Impact:** Victims may suffer identity theft, financial fraud, and security compromise.

2.3.2 Confusable Domains (Typosquatting)

- **Description:** Registering domain names that look visually similar to popular websites, taking advantage of typing errors or character similarities ?.
- **Mechanism:** Users may accidentally visit these websites when making a typo in a URL, which can expose them to malware or phishing attempts.
- **Impact:** Deception of users and potential harm to brand reputation ?.

2.3.3 Domain Hijacking

- **Description:** Unauthorised acquisition of domain names by exploiting security vulnerabilities in the domain registration system ?.
- **Mechanism:** Attackers may use tactics like social engineering, phishing, or exploiting security loopholes to gain control over a domain.
- **Impact:** Loss of control of the website, redirection to malicious sites, and potential data breaches.

2.3.4 Botnets

- **Description:** Botnets involve controlling a group of computers infected with malware, used to carry out attacks or spread spam and malware ?.
- **Mechanism:** Malware infects computers of unsuspecting users, incorporating them into a network under the attacker's control.
- **Impact:** Can result in large-scale DDoS attacks, mass spam campaigns, and widespread malware dissemination.

2.3.5 Fast Flux Hosting

- **Description:** A technique used to conceal the location of websites associated with phishing and malware distribution ?.
- **Mechanism:** Involves a network of compromised hosts that regularly modify DNS records to avoid detection.
- **Impact:** Makes tracking and shutting down malicious sites difficult.

2.3.6 Domain Generation Algorithms (DGA)

- **Description:** DGAs generate domain names that act as meeting points for botnets ?.
- **Mechanism:** Malicious software uses algorithms to generate a sequence of domain names for command-and-control servers.
- **Impact:** Adds complexity to efforts to disrupt botnet command and control channels.

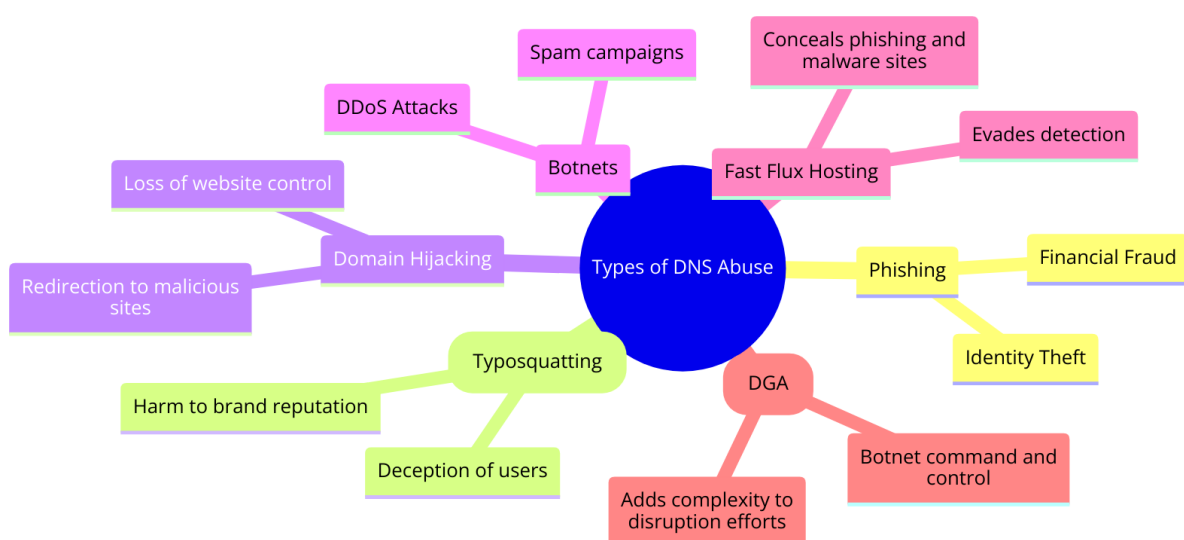


Figure 2.1: Different Forms of DNS Abuse.

2.4 How DNS Abuse Harms Users

DNS abuse has serious and detrimental effects for both users and organisations, going beyond basic technological disruptions. Identity theft is among the most direct and direct effects. Phishing attacks, a common type of DNS abuse, use realistic websites to trick visitors into revealing sensitive data. Such attacks can produce information that results in financial theft, unauthorised access to accounts, and long-term damage to a person's reputation and credit ?.

2.4.1 Identity Theft

- **Phishing:** Phishing attacks often use domain names that imitate legitimate websites, fooling users into providing sensitive information such as usernames, passwords, or financial details, leading to potential identity theft.

2.4.2 Financial Loss

- **Deceptive Transactions:** Users may be tricked into making payments to deceptive websites or unknowingly disclose their credit card information, resulting in financial losses ?.

2.4.3 Data Breach

- **Malware:** Malicious software spread through compromised DNS systems can allow unauthorised access to corporate data, leading to data breaches ?.

2.4.4 System Compromise

- **Malware Infection:** Systems infected with malware due to DNS abuse can be exploited for further attacks, including the creation of botnets or the distribution of ransomware, resulting in system compromise ?.

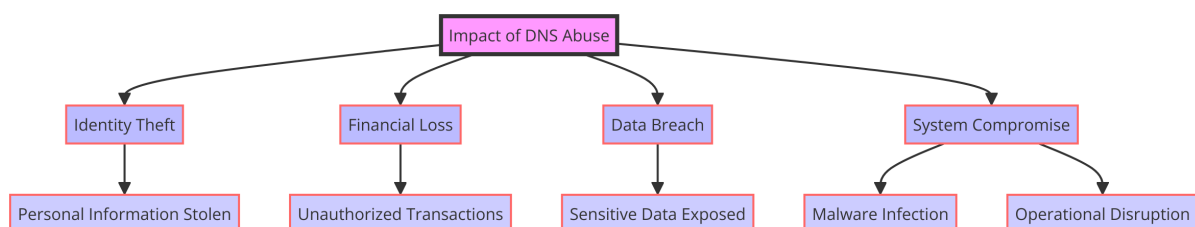


Figure 2.2: How DNS Abuse Harms Users.

2.5 Future Dangers of DNS Abuse

As technology develops, so do bad actor strategies and tools, creating a dynamic environment for DNS abuse that could present new risks in the future. The sophistication of attacks has increased, which is a major issue. Bad actors are always creating increasingly sophisticated methods to take advantage of DNS, such as creating more convincing phishing schemes and using advanced virus distribution networks ?.

2.5.1 Increased Sophistication

- **Evolving Techniques:** Bad actors are constantly developing more sophisticated techniques to exploit DNS, such as advanced phishing schemes and malware distribution ?.

2.5.2 IoT Vulnerabilities

- **Expanding Vulnerabilities:** The widespread adoption of Internet of Things (IoT) devices, which often lack robust security measures, presents a growing target for DNS-based attacks ?.

2.5.3 Infrastructure Attacks

- **DNS as a Prime Target:** Attacks on DNS infrastructure can disrupt internet services on a large scale, including DDoS attacks targeting DNS providers or exploiting weaknesses in DNS protocols ?.

2.5.4 Deepfakes & AI

- **AI-Enhanced Phishing:** The use of AI technologies, such as deepfakes, has made phishing attacks more convincing and deceptive, manipulating audio and video content to impersonate trusted entities ?.

2.5.5 Cloud Computing Vulnerabilities

- **Targeting Cloud Services:** As organisations increasingly rely on cloud-based services, bad actors are exploiting DNS vulnerabilities to attack these platforms, potentially leading to data breaches and service disruptions ?.

2.5.6 Mobile Device Exploitation

- **Mobile DNS Attacks:** The rising usage of mobile devices has led bad actors to target smartphones and tablets through DNS-based attacks, which can lead to data theft and the spread of malware ?.

2.5.7 Cryptocurrency & Blockchain Exploitation

- **Crypto-Related DNS Attacks:** Attackers could exploit DNS vulnerabilities to redirect users to fake cryptocurrency exchanges or blockchain platforms, leading to financial fraud and theft of digital assets ?.

2.5.8 Political and Information Warfare

- **DNS in Cyber Warfare:** The manipulation of domain name systems can be used to spread misinformation or disrupt services during significant political events, serving as a tool for political and information warfare ?.

2.5.9 Exploiting Emerging Technologies

- **Abuse in New Tech Domains:** As new technologies such as 5G, AI, and quantum computing advance, tactics involving DNS abuse are likely to evolve, potentially leading to more sophisticated attacks ?.

2.5.10 Supply Chain Attacks

- **DNS in Supply Chain Compromise:** DNS manipulation can also be employed as part of supply chain attacks, targeting software updates or cloud-based services to compromise organisations ?.

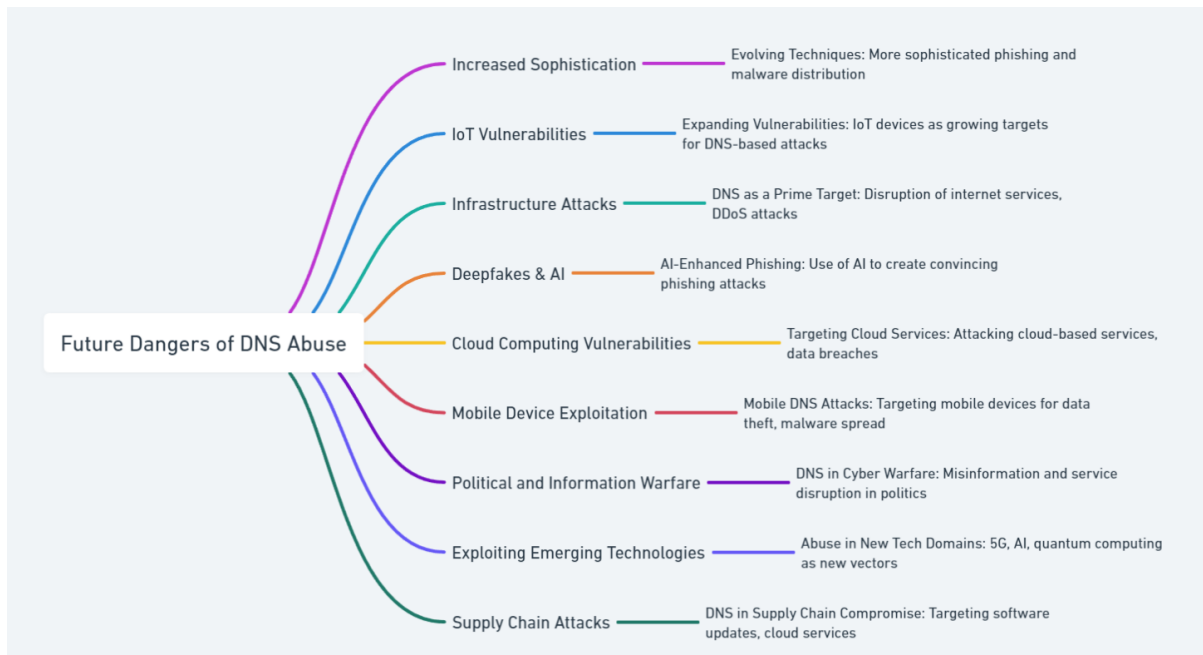


Figure 2.3: Future Dangers of DNS Abuse.

By understanding these future dangers and emerging trends, stakeholders can better prepare and adapt their strategies to anticipate and counteract the evolving nature of DNS abuse.

2.6 Foundational Mitigation Strategies & Best Practices

To address the broad nature of threats, mitigating DNS abuse requires an integrated strategy that integrates multiple strategies and best practices. The establishment of reporting and monitoring procedures is one fundamental tactic. Automated systems have the ability to track domain name registration patterns that may indicate DNS abuse, and protocols to report questionable actions can help ensure prompt intervention ?. To confirm security and ensure that systems have not been compromised, regular audits of DNS configurations and domain registrations are also necessary ? .

1. Monitoring & Reporting

- Implementation: Use automated systems to monitor domain name registration for patterns that may indicate DNS abuse ?. Establish procedures for reporting activities to authorities or cybersecurity organisations ?.

2. Security Awareness Training

- Implementation: Develop training programmes for users and IT staff with a focus

on recognising phishing attempts, practising browsing habits, and understanding DNS security.

3. DNS Security Extensions (DNSSEC)

- Implementation: Deploy DNSSEC to ensure the integrity of the DNS data. This involves signing DNS records to protect against modification and DNS spoofing.

4. Multi-Factor Authentication (MFA)

- Implementation: Enforce multifactor authentication (MFA) for domain registrars and interfaces used to manage DNS ?. This adds a layer of security beyond passwords, helping to prevent unauthorised domain transfers or alterations ?.

5. Blacklisting & Takedown Services

- Implementation: Collaborate with cybersecurity firms to identify and blacklist domains engaged in malicious activities. Establish response teams dedicated to removing domains involved in DNS abuse.

6. Collaboration

- Implementation: Foster collaboration among Internet service providers (ISPs), domain registrars, governments, and cybersecurity organisations. Share intelligence and best practices to collectively improve defence against DNS abuse ?.

7. Regular Audits

- Implementation: Conduct security audits of domain registrations and DNS configurations to verify their security and ensure that they have not been compromised ?.

8. Machine Learning

- Implementation: Using AI and machine learning algorithms to analyse patterns in DNS traffic and proactively predict instances of DNS abuse ?. This proactive approach enables the identification of threats before they materialise ?.

9. Geo-Blocking & IP Filtering

- Implementation: Deploy geo-blocking and IP filtering techniques to limit access to DNS services from regions that have a history of DNS abuse. This can reduce the risk that attackers will use these services to carry out malicious activities or distribute malware ?.

10. Enhanced Domain Validation Procedures

- **Implementation:** Enhance the domain registration process by implementing validation procedures. This may involve verifying the identity of individuals or organisations that register domains, especially domains that resemble brands or fall into sensitive categories. By taking these measures, we can strengthen security and mitigate the risks associated with fraudulent domain registrations.

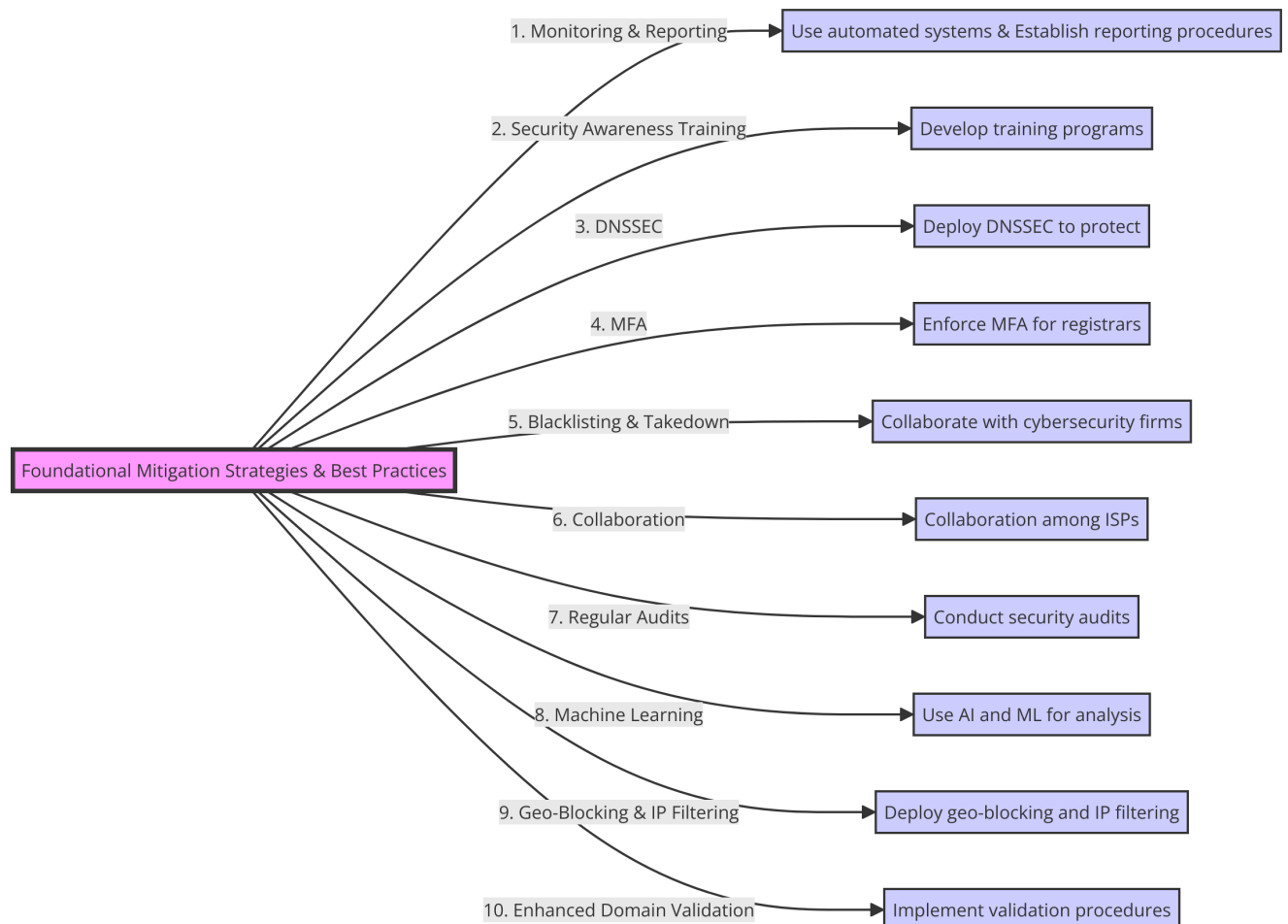


Figure 2.4: Mitigation Strategie.

Each of these strategies plays a role in creating a comprehensive defence against DNS abuse. By integrating these tactics, organisations can establish robust, proactive measures to detect, prevent, and mitigate the ever-evolving threats posed by DNS abuse.

2.7 Summary & Synthesis

After exploring the different forms of DNS abuse , How DNS abuse harms user , Future Dangers of DNS abuse and Mitigation Strategies and Best Practices. I have designed a table that has DNS abuses and the best possible mitigation strategies to help them against them, taking into account the transparency story behind it , user harm and reasoning.

DNS Abuse	User Harm	Mitigation Strategy	Reasoning	Transparency Aspect
Phishing	Identity Theft, Financial Loss	Security Awareness Training, Enhanced Domain Validation Procedures	Training helps users recognize phishing attempts. Validation prevents registration of mimic domains.	Increases awareness and scrutiny during domain registration.
Confusable Domains (Typosquatting)	Unauthorised Account Access	Enhanced Domain Validation Procedures, Regular Audits	Prevents Registration of Similar Domains. Audits ensure compliance.	transparent domain registration process.
Domain Hijacking	System Compromise, Data Breach	Multi-Factor Authentication (MFA), Regular Audits	MFA secures domain management. Audits verify security measures.	Accountability in domain management.
Botnets	Malware Distribution	Collaboration, Machine Learning	Intelligence Sharing identifies botnet activities. AI predicts the formation of botnets.	Shared responsibility and proactive detection.
Fast Flux Hosting	System Infections	Blacklisting and Takedown Services, Geo-Blocking	Rapid response to malicious domains. Restrict access from risky regions.	Responsive and transparent threat management.
Domain Generation Algorithms (DGA)	Malware Distribution	Machine Learning, DNS Security Extensions (DNSSEC)	AI detects abnormal patterns. DNSSEC prevents spoofing.	Integrity and trust in DNS data.
IoT Vulnerabilities	Unauthorised Access, Data Breach	Security Awareness Training, Collaboration	Educates on security practices. Collaboration on best practices.	Open exchange of knowledge and efforts.
Infrastructure Attacks	DDoS Attacks, System Downtime	DNSSEC, Collaboration	Protects DNS data integrity. Sharing of threat intelligence.	Collective action strengthens the DNS infrastructure.
Deepfakes and AI	Identity Theft, Misinformation	Security Awareness Training, Monitoring	Recognising Phishing. Monitor AI threats.	Vigilance and prompt threat reporting.
Cloud Computing Vulnerabilities	Data Breach, Unauthorised Access	Regular Audits, Enhanced Validation	Secure DNS settings in cloud services. Prevents exploitation.	Framework for secure domain use in cloud.
Mobile Device Exploitation	Unauthorised Access, Financial Loss	MFA, Security Awareness Training	Secures account access. Raises awareness of threats.	Mobile security awareness and protection.
Continued on next page				

DNS Abuse	User Harm	Mitigation Strategy	Reasoning	Transparency Aspect
Political and Information Warfare	Misinformation, Political Manipulation	Monitoring, Collaboration	Monitoring abuse in campaigns. Unified response to misinformation.	Transparency in monitoring and collective action.
Exploiting Emerging Technologies	system Vulnerabilities	Machine Learning, Collaboration	Analytics to predict DNS abuse. Share knowledge about threats.	Innovation in defense strategies and sharing.
Supply Chain Attacks	System Compromise, Data Breach	Regular Audits, Blacklisting	Audits for DNS integrity. Rapid response to threats.	Transparency in supply chain security.

Table 2.1: Mitigation strategies against DNS abuse and its impact on users.

Finally, this chapter has examined all aspects of DNS abuse, the various forms, the serious harm it does, as well as potential future threats. To create efficient regulations and countermeasures, it is essential to understand the extent and consequences of DNS abuse. Significant progress towards resolving these issues has been made by organisations like the DNS Abuse Institute and ICANN. However, as new technologies are incorporated into the equation and the threat environment changes in sophistication, it becomes increasingly important to adopt alert, flexible and cooperative strategies. The mitigation techniques and best practices discussed in this chapter provide a roadmap for mitigating DNS abuse. Every tactic contributes to a defence mechanism, from advanced technology solutions and improved methods for validation to monitoring and reporting. It is impossible to overestimate the value of cooperation, regular checks, and the application of cutting-edge technologies to anticipate and mitigate DNS abuse. After analysing the data, it is evident that a team effort is needed to comprehend, track, and mitigate DNS abuse. A complex strategy that integrates multiple techniques and encourages collaboration across industries is required instead of a single insufficient strategy. Our approaches to preserving the integrity and security of the DNS and, consequently, the larger Internet infrastructure must adapt, as does the digital environment.

By understanding the connections between different aspects of DNS abuse and reinforcing the collective effort required for effective mitigation, stakeholders can be better prepared to face the challenges ahead. This chapter sets the stage for further research and action, with the aim of contributing to a safer and more secure digital world.

3 State of the Art

This chapter explores the strategies used to mitigate DNS abuse and new developments in this field. Explore and evaluate the effectiveness and transparency of multiple mitigation techniques, including DNS filtering and threat intelligence, in which experts organise and analyse information about cyber attacks. Additionally, the use of domain-generating techniques and DoT and DoH are two novel forms of DNS abuse that are highlighted in this section. In addition, the role of AI and machine learning in identifying and mitigating DNS abuse is covered. The final half of the section includes a discussion on potential future research areas and technologies to improve DNS abuse mitigation. Case studies offer practical information on DNS abuse occurrences.

3.1 Current Strategies and Their Effectiveness in Relation to DNS Abuse

DNS abuse presents a significant challenge for Internet entities involved in domain name management. Various approaches are employed to mitigate such abuse, including DNS filtering, which regulates access to specific websites and prevents you from accessing malicious sites that can administer phishing and ransomware. Additionally, threat intelligence methodologies use data analysis to identify potential risks, as exemplified by ?. Anomaly detection plays a role in identifying suspicious DNS activities indicative of malicious intent using Packet Analysis to analyse individual packets for DNS allowing for real-time detection and statistical analysis, which involves performing statistical analysis on a large dataset of DNS traffic. However, these methods can face operational challenges, such as errors and the need for fast access to critical threat data.

3.1.1 Transparency in DNS Abuse Mitigation & DNS Relevance

1. A Case Study of Cloudflare's Transparency Approach

Cloudflare is committed to maintaining transparency ?, which is the keystone of their relationship with customers, guiding each of these approaches to reports of abuse of

the DNS and requests that may come from law enforcement. All of these reduce their actions and policies in moulding a trustworthy environment in light of addressing Internet safety and privacy concerns. Their approach to handling DNS abuse reports and law enforcement requests is anchored on three core principles:

- (a) Require due process: Cloudflare will comply with due process as required by law, remaining neutral and not exceeding legal requirements.
- (b) Respect privacy: Cloudflare respects your privacy and will never sell or otherwise share any personal or private information with any third party without your explicit permission. This is applicable to each and every request.
- (c) Provide Notice: Cloudflare will notify customers if legal requests are made for their information, unless prohibited by law.

The Cloudflare Transparency Report gives deep statistics and trends based on DNS abuse reports on Cloudflare's response:

- (a) Abuse Reports: Cloudflare actively responds to abuse reports, including phishing, malware, and copyright infringement.
- (b) Actions taken: Cloudflare may terminate services for domains involved in abuses such as phishing or malicious activities.
- (c) Termination of services: 206 accounts and 530 domains are suspended for the latter half of 2022 for hosting domains associated with CSAM that were not compliant with reported issues.
- (d) UDRP Requests: Cloudflare responded to 21 UDRP (Uniform Domain Name Dispute Resolution Policy) requests from an ICANN-approved dispute board in the second half of 2022.

In addition , Cloudflare's careful description of compliance and due process with respect to handling law enforcement requests comes from their latest Transparency Report. Below is a summary of the major areas covered.

- (a) Legal Sufficiency Review: Cloudflare reviews the legal validity of requests before taking any action according to the law and respects the privacy of the users. Cloudflare responds only to valid law enforcement requests, including court orders and subpoenas.
- (b) Respect to International Privacy Laws: Cloudflare checks the disparity of the request, rejecting to honour it if it is at odds with the rights enshrined by the privacy laws of the two countries.
- (c) Emergency disclosure requests: Cloudflare only considers making emergency

disclosures to law enforcement where there is an imminent danger of harm and clearly requires a stated intention for the follow-up of legal processes.

- (d) National Security Requests and Non-Disclosure Obligations: National security orders are incompatible with the company's aims of transparency; thus, Cloudflare is challenging them.
- (e) International Requests for Data: Cloudflare reviews such requests from the foreign government in accordance with the United States legal process or on a case-by-case basis consistent with international norms and policies.
- (f) Challenging Overly Broad or Inappropriate Requests: Cloudflare may object to and help our customers fight overly broad or inappropriate requests from law enforcement as a matter of transparency and user rights. USA.

Public reporting by Cloudflare and working closely with law enforcement, as well as other partners, form important elements in its strategy of mitigating DNS abuse such as:

- (a) Reporting to the Public & Transparency: Cloudflare opens its data to the public to showcase the types and the volume of abuse reports for trust-building and to exemplify the notion of efforts against antiabuse.
- (b) Law Enforcement Cooperation: Cloudflare partners with law enforcement regarding the privacy of citizens in such a way that it makes sure the proper legal justification of the actions in relation to DNS abuse.
- (c) Mitigation actions: Cloudflare makes a proactive effort to prevent DNS abuse by stopping access to any offending domains that are used in phishing, malware distribution, and other damaging activities.abuse.
- (d) Challenges to Mitigating DNS abuse: Cloudflare admits to striking a balance between free speech, legal matters, and the need for stakeholders' joint efforts in the quest to fight DNS abuse.
- (e) Efficiency of Efforts to Mitigate DNS Abuse: Although successful mitigation involves tackling the root causes and diversity within the market, Cloudflare's transparency reports help in understanding abuse mitigation efficiency.

Some of the challenges the Transparency Report showcases that Cloudflare is grappling with the complexity of DNS abuse, how to achieve a balance between transparency and privacy, and being legally and regulatory compliant, besides also having technical limitations in the mitigation of misuse. This allows ideas to be used to improve processes.

- (a) **Enhanced Cooperation with Stakeholders:** Cloudflare proposes that such a relationship with law enforcement, service providers, and international organisations will be an industry best practice to standard procedures to increase the efficacy of the internet by mitigating DNS abuse.
- (b) **Improve Abuse Detection Systems:** Cloudflare said it would invest its capital in funding more development in advanced technologies, machine learning, and further enhancement of abuse detection systems to allow for faster identification and mitigation of abusive content.
- (c) **Transparency Reporting Enhanced:** Cloudflare looks forward to providing even more granular transparency reports that would give deep insight into the types of abuse on DNS and the effectiveness of its mitigation for improved abuse handling practice.
- (d) **Better User Education & Awareness:** The focus is to develop more educational materials and programmes to inform the user, bringing to their notice the risks of cybersecurity and DNS abuse for a safer Internet environment.
- (e) **Advocate Policy and Legal Reforms:** Cloudflare works to propose and advocate policy and legal reforms, which could be embraced in mitigating any potential collision points between privacy laws and law enforcement requests, hence balancing user privacy with the fight against DNS abuse.
- (f) **Create a Multi-stakeholder Feedback Mechanism:** A mechanism can be put in place that ensures feedback not only from the users but also from the civil society and other stakeholders; that would bring out to what extent Cloudflare was able to be successful in their efforts towards transparency and reduction of abuse. Such recommendations can be useful for guiding any further policy-making or organisational policy enhancements.
- (g) **Continue to Challenge Over-broad Requests:** The company does not even go on to commit to resisting overbroad or inappropriate requests for data; the user's rights and due processes are put above all others, which would not help harden their service as a trusted industry leader.

In conclusion, the company emphasises its commitment to protecting legal processes and user privacy while navigating government and law enforcement requests. A critical aspect of these reports is Cloudflare's approach to DNS requests, particularly regarding content blocking through its 1.1.1.1 Public DNS Resolver. This was the key answer: Cloudflare, in no uncertain terms, "received legal requests to block content at our DNS servers" and stated its policy to first "exhaust legal remedies" that they could enforce. This is an indication of how very carefully Cloudflare has to adhere to the

demands of the law, yet protect the openness of the Internet, bringing out just how major DNS is in all matters that pertain to the accessibility of content on the Internet and governance of the Internet.

2. Google Transparency Reports

This shows the weight attached to the Domain Name System (DNS) when enforcing the requests from the global governments, more so in between them and the internet governance, in relation to the content removal from Google services. Data from Russia, with tens of thousands of redaction requests, might signal broader actions that include DNS-level interventions. This highlights the kind of role DNS plays in controlling access to the Internet or blocking content, which is usually put under legal and regulatory pressures from major tech companies, including Google.

Any question related to these requests, although not directly related to the manipulation of DNS, implies the possibility of any technical adjustment to be carried out in order to fulfil the criteria directly affecting DNS resolutions. This indirect reference considers DNS to be one of the critical infrastructures in the debate on Internet governance, censorship, and access to information. What it does is show the Google Transparency Report, which indicates the fact that DNS is an important architecture of the Internet and is also a trouble spot for exercising control over digital content and information flow ?.

3. Amazon Transparency Reports

Necessarily, such a role of DNS in servicing governments or other legal data demands does not trace directly to specific acts of manipulation in the DNS or intervention at the domain-level. The report explains about Amazon's observance of due process laws in handling requests for data such as subpoenas and search warrants, with a lot of emphasis on customer privacy and protection of data which can be mounted against the state or any other third party institution or person. It goes without saying that handling the domain or the services to do with this website means that a possibility of such a move as DNS changes can be in the offing. However, they do not give clear examples where DNS interventions have been taken, but describe the circumstances related to legal compliance and internet governance without direct reference to DNS ?.

4. DNS- SB Transparency Reports

xTom reported nil compliance, for the most part, within the international statistics of content data requests, requests for information on subscribers, requests to have content taken down, requests to have content blocked, and domain name dispute resolutions in 2020. These zero compliances are placed to highlight the fact that the organisation, in reality, sets the protection level of user data and content integrity too

high, which is part of a general position on how DNS and domains are managed for the protection of users and the achievement of operable thresholds ?.

5. The CyberGhost Transparency Report

An obvious upward trend of the recursion without DMCA complaints, along with flagging malicious activities, flashes up in each year, record by record, before a sudden spike around 2023. Given the growing level of claims and requests, CyberGhost still regards the No Logs policy as a strong sweat so they keep a keen eye and hence stays guardedly strong on the user's privacy and any request relating to DNS. The report is categorical with such an idea that even in the case of mitigating malicious activity, they do not involve logging of DNS queries or respective user activity; therein, the integrity of user data and an assurance towards compliance in privacy. DNS somehow plays a function in this case: It becomes evident that the design of the CyberGhost infrastructure is supposed to be resistant to infiltrators and, hence, capable of withstanding invasions and pressures in no less than those that would compromise an individual's anonymity and right to freely receive information via the Internet ?.

6. The Meta-Transparency Reports

At the same level of social media, the enforcement of intellectual property rights, including Facebook and Instagram, shall entail the enforcement of a comprehensive strategy targeting copyright, counterfeit, and trademark infringements, with an important focus on the Domain Name System (DNS) as the centre stage for such activities. The DNS serves both as a foundation for the distribution of information on-line and as a checkpoint in the enforcement process. For example, content removals from Facebook and Instagram amount to 447,123 and 297,356, respectively, in the first half of 2022. This shows a scenario in which interventions range from more than platform moderation to include DNS-level actions of deindexing websites or altering DNS records to block access to infringing content.

The sustained rate of content removals since the latter halves of 2020 and 2021 indicates a reliance on DNS mechanisms. This may explain the huge year-over-year drop in Facebook's copyright and counterfeit content takedown requests from 2020-2021. It would seem that Meta (the parent company of Facebook) may not work with DNS providers to have the offending domains taken down, but instead remove the infringing content. This underscores how important DNS is in the enforcement of intellectual property rights, the checks on the spread of the counterfeit, fake, and grey markets, and in protecting the rights of the owner of intellectual property and trademarks ?.

7. T-Mobile Transparency Report

It outlines how the company complies with directions of the law in the management of requests for information from consumers, thus highlighting staying within customers' privacy and legal compliance. Details the approach and policies of the company in response to lawful requests on records of customers within T-Mobile, Metro by T-Mobile, and Sprint, now collectively T-Mobile USA, Inc. (TMUS). At the same time, it provides information about what TMUS does to protect consumers from unauthorised data access, including first-party requests made by the company itself, such as subpoenas, court orders, and warrants, with all processes required following the same. When sharing details surrounding the number and types of requests received in 2022, the report marks a heavy emphasis on TMUS's efforts to take care of customer privacy and complying with applicable legal obligations. In the case of T-Mobile, it handled 301,388 subpoenas, mostly related to orders to disclose information about the subscriber, such as names and addresses, and 94,599 different types of warrants or search warrants, which can be after historical location data or the content of messages ?.

8. IBM 1H 2021 Law Enforcement Requests Transparency Report

IBM focuses on data ethics and transparency, just as it has done throughout the years to build trust among clients. The emphasis is on who owns the data and promotes client data policies, belonging to the government, and being fair and not discriminatory. The IBM report aims to make it clear where the company stands on the issue of client data that go through government surveillance. Therefore, it advocated that governments make their request for information directly to the client and ensure that the engagements between them are strictly regulated by legal protocols, including Mutual Legal Assistance Treaties (MLATs). IBM received 27 law enforcement requests in the first half of 2021, most of them related to the provision of basic subscriber contact information. It underpins how rarely and seriously IBM views requests for customer data. This reflects how IBM is committed to client privacy and data protection by ensuring strict controls in relation to data access, including those prompted by legality and governance ?.

9. Trade Me Transparency Report

The Trade Me report underscores its promise to be candid and open with detailed accounts of dealing with the agencies of the New Zealand Government. This is its 11th annual disclosure. The report demonstrates an effort of Trade Me to strike a balance between legal obligation and privacy of its members by making proactive disclosures of member information to government bodies, establishing transparency, and upholding their values. This stands as a testimony to the very careful process of Trade Me's Trust and Safety team, ensuring the legality and necessity of information

released in the aim of maintaining community safety within legal bounds. This practice develops confidence in members in each other and makes the online environment feel safer. Importantly, it provides a specific number of government data requests and disclosures for the year ended June 2023, revealing that Trade Me is keeping the discussion about government access to data open. For example, it refers to a 36% reduction in the release of voluntary information to the New Zealand Police, which describes the caution of the company in terms of voluntary information release ?.

10. Xiaomi Transparency Report: Government Requests for User Information (2022)

It indicates how Xiaomi processes user data requests from the government and testifies to this company's determination towards transparency and legality. Strives to follow technical and organisational practices set as standards within the industry in the world and full respect for the laws and regulations. This general review portrays Xiaomi as a transparent organisation in the way it handles various requests from the government, from the device level to financial and account-based data, underlining the trust that Xiaomi has built with consumers regarding their privacy and data protection. In 2022, there were 51 device-based requests, among the many applications received by the Indian government. Among the device inquiries, 49,683 devices were answered, with 32 in compliance. The Xiaomi compliance rate in India reached an impressive 62. 75%. It is indicative of the fact that the company is usually under huge government inquiries from regions where it has big stakes and shows the nature of the requests that this company has always faced ?.

11. eBay Global Transparency Report

The report is a demonstration of eBay's commitment to making the marketplace safe and reliable for the global community of buyers and sellers transacting on its platform. Defined with great focus, eBay lists everything they are doing to protect their marketplace from counterfeit goods, fraud, and any other abuse. With advanced AI technologies and image detection, eBay will be able to identify and remove listings of goods that could pose risks to safety or health, with close follow-up efforts to improve cooperation with rights owners and law enforcement. They are included in measures within the scope of eBay investments in technology and partnerships towards the retention of platform integrity. Reflecting the policies and their impact on the initiatives of the company for more than two decades, the report has highlighted that eBay believes in creating an open and honest marketplace that can help individuals generate economic opportunities from across the world. eBay AI tools had proactively stopped 295 million listings of prohibited items during 2022, a clear indication that its technology is very key to stopping the sale of controlled substances and other damaging items. On the other hand, the Authenticity Guarantee programme further

underlines the quality consciousness of eBay and builds trust by allowing verification services for luxury offerings, which include watches, handbags, jewellery, sneakers, and cards ?.

12. Cisco Transparency Report: Government Data Demands (First Half of 2023)

The report underscores Cisco's stated commitment to providing transparency about government requests for customer data around the world. This is an important lens into the world of data privacy and government surveillance, outlining the amounts and kinds of request for content and non-content data being made. The publication of compliance, rejections, and all cases in which data was not found shows the effort to balance legal obligations with the privacy of the customer. In particular, it is in compliance with national security demands, in accordance with the United States Freedom Act of 2015. According to the company's reports, during the specified period, Cisco received 16 demands from the US government agencies regarding non-content data and disclosed it in 7 cases. For this period, the company recorded a compliance rate of 44% non-content data requests (NCDR). It is from such data that a comprehensive illustration of how Cisco handles government requests for data can be shown to have the regard given to government interests or balance with privacy rights. It also points to international involvement, where of the 27 requests from Germany, 25 were disclosures, therefore showing the extent and scope of the interest governments have in data ?.

13. Apple Transparency Report : Government & Private Party Requests

It details the process by which Apple's legal team handles all legal requests from global government agencies and US private parties, categorising them by Devices, Financial Identifiers, and Accounts. This highlights the process that Apple undertakes with all the devotion to the protection of user privacy and information safety, at the same time dealing with the requests within legal standards. This commitment to transparency is aimed at building trust and informing opinions about Apple's operations. The report is key for any reader who is interested in understanding at a more detailed level the intersections of technology, privacy, and law enforcement in the digital age. The information describes the types and volumes of requests in which, for example, Apple reports having received 5,660 device requests in the US and reports that have furnished information for 82% of these requests, mostly associated with investigations of lost or stolen devices or fraud. The U.S. posted a total of 7,944 account requests, with a disclosure rate of 47%. This clearly proves that Apple has been pretty guarded in its responses to requests for user data. ?.

3.1.2 Effectiveness of Current DNS Abuse Mitigation Strategies

Different methods are used to mitigate DNS abuse, including the implementation of blocking tools, awareness of potential threats, and identification of anomalous behaviour. DNS filtering entails the regulation of website access based on predetermined rules, which can have varied outcomes depending on the context in which it can happen in different environments such as register and registry in which it implements mechanisms to compare DNS names to the block list and given set of rules then takes the necessary action such as homograph attacks in which DNS filtering mechanism play a role in mitigating them by comparing domain names against block lists and predefined rule to identify potentially malicious homographs as stated earlier. Threat intelligence plays a role in identifying potential dangers and detecting unusual activities within the DNS, as noted ?, such as allowing proactive identification and assessment of potential threats and malicious activities, including detecting patterns indicative of phishing, domain hijacking, malware distribution, and other forms of DNS abuse. Evaluating the effectiveness of these methods requires careful consideration of their performance in real-world scenarios. For example, while DNS filtering can effectively block malicious content, it may inadvertently permit harmful elements to bypass the filtering process, potentially impacting the user experience. Similarly, the effectiveness of threat intelligence relies on the timeliness and accuracy of the data used. However, identifying anomalous behaviour poses challenges, as distinguishing between malicious actions and legitimate activities performed in innovative ways can be challenging.

3.2 Emerging Trends in DNS Abuse

Trends in DNS abuse had declined among some categories, such as botnets, malware, phishing, and spam. Much of this decline could be attributed to the multipronged approaches that ICANN itself launched around data analysis, community tools, and enforcement of registry and registrar obligations ?. Although continuing to be slow, adopting organisations did so under the compulsion of situations that left them no choice but to use technology or by those for whom TLS adoption was a matter of technological innovation, choice, or desire for the embrace of technologies simpler and more robust from misdirection. One of the major issues has continued to be privacy, due to the fact that DNS queries have been accidentally found to give away user behaviours. One such move to enhance user privacy is the Query Name Minimisation. The main concern has been how to remain vigilant against DNS abuses while improving privacy without altering service efficiency.

3.2.1 Evolving New Forms of DNS Abuse

The field of cybersecurity is rapidly advancing, bringing forth new challenges as it evolves, and constantly moving the goalposts for defence mechanisms. The introduction of DNS over TLS (DoT) and DNS over HTTPS (DoH) is like a double-edged sword. Although these encryption protocols were designed to enhance privacy and security by encrypting DNS queries, they unintentionally provide attackers with means to disguise malicious traffic. This expands the attack surface, affecting everything from individual devices to corporate networks. For example, attackers could take advantage of DoT and DoH in enterprise settings to avoid outdated security controls and establish hidden communication channels. Furthermore, Domain Generation Algorithms (DGAs) play an important role in cyber threats by automatically generating a large number of random domain names, making it extremely difficult to identify and shut down malicious sites. This tactic, integral to botnet command and control (C2) operations, significantly complicates cybersecurity defence efforts to predict and mitigate threats.

The adoption of DoT and DoH offers several benefits, such as enhanced privacy by preventing the surveillance of DNS queries and improved security through the encryption of DNS traffic, which weakens hackers' attempts to intercept or manipulate data. However, these protocols also allow attackers to hide their malicious activities, which poses challenges for traditional DNS security systems in detecting and filtering harmful content. Furthermore, these protocols could accidentally bypass content filtering policies, leading to potential security breaches within organisations. Conversely, DGAs provide attackers with a method to evade detection and maintain C2 communications, as the dynamically generated domains are difficult to predict and preemptively block. This results in an overwhelming number of domain names for security mechanisms to monitor, complicating the threat intelligence process and necessitating continuous vigilance and blacklist updates. The widespread adoption of these technologies underscores the need for cybersecurity professionals to adopt a proactive and informed stance, understand their potential for exploitation, and develop comprehensive strategies. These strategies must strike a balance between the benefits of encryption and domain generation and the imperative to prevent DNS abuse, ensuring the integrity and security of the online environment.

3.2.2 Predictive Measures & Their Transparency

Efforts to mitigate DNS abuse are set toward immediately slowing such activities by utilising complex systems and advanced machine learning algorithms to detect patterns indicative of DNS abuse. Articulating and sharing insights about the decision-making processes in predictive modelling is considered significant, as well as the efforts by registrars and registries, acting together, in the context of DNS Abuse Transparency are comprehensive.

These entities will invoke a wide range of mitigation measures to minimise damage and losses related to DNS, which will ensure the development of a more secure and trusted Internet environment. Some key mitigation strategies are account-based remediation in the way that maliciously generated accounts are locked out and further validated, in addition to monitoring third-party feeds and reports from cybersecurity organisations, law enforcement, and the public to discover and address abuse early. Moreover, this mitigation involves malware analysis, which comes from attacks on the communication infrastructure and the corresponding IP addresses, through suppression or sinkholes in the context of botnets and the use of domain generation algorithms (DGA) that direct botnet traffic ?. Most specifically, sinkholing is an authoritative measure that directs traffic from abusive domains to harmless servers and allows studies to be conducted on the sources of traffic and the extent of compromise. Compliance with legal and contractual requirements further underscores the actions of registrars and registries against DNS abuse, ensuring that their actions in mitigation are within the context of the ICANN agreements and local laws.

The evident evaluation of real-time black hole lists (RBLs), in addition to the responsible role of trusted notifiers, further increases the effectiveness and accuracy of mitigating actions, to filter and validate reports on abuse, so that proper responses may be made. This multipronged approach on the part of the registrars and the registries towards the mitigation of DNS abuse does not only emphasise the proactive and reactive measures, but also the possibilities of increased transparency as far as reporting and publicising the actions in place against DNS abuse are concerned. Such transparency is key to building trust, open to accountability, and creating an environment conducive to stakeholders' collaboration for the more effective fight against abuse in the DNS ecosystem. This transparency helps to understand the rationale behind the predictions, map the data used for model training, and clarify the methods that guide decision-making, as highlighted in ?. Striking a balance between the complexity of predictive models and their interpretability is a significant challenge. Therefore, it is essential to approach this challenge with caution, ensuring that the models are not only effective in identifying DNS abuse but also accessible for thorough examination and accountability.

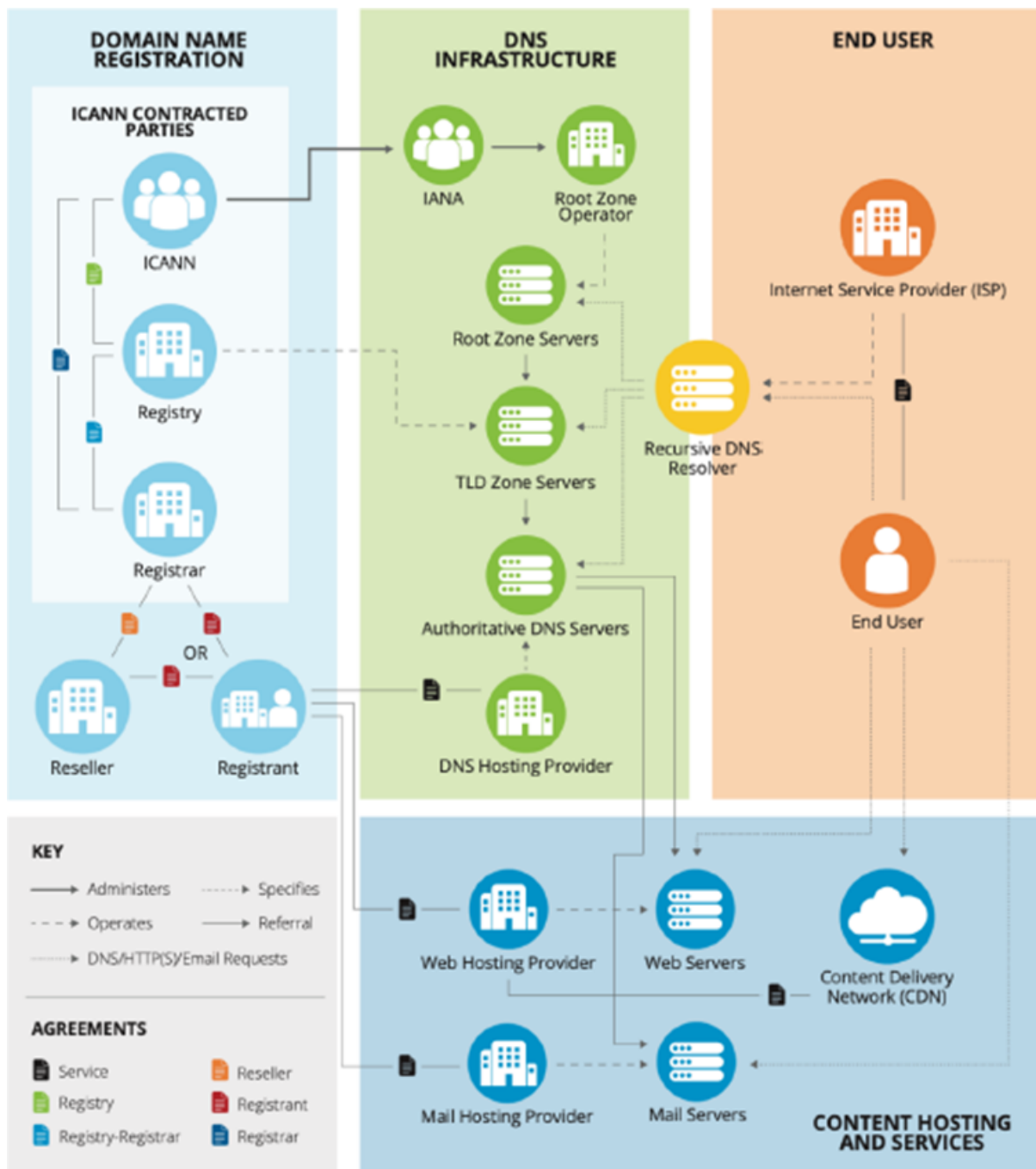


Figure 3.1: DNS Ecosystem Contractually Related to ICANN (image courtesy of Verisign and originally published in SSAC 115 adapted from ?)

3.3 Technological Advancements

The mitigation of DNS abuse is increasingly influenced by the integration of artificial intelligence (AI) and machine learning technologies ?. At the helm of this evolution are innovative tools such as the iQ Domain Risk Score, which employs machine learning and string analytics to proactively detect potential domain abuses now of registration ?. This tool aims to act as a mitigation measure by analysing domains against criteria indicative of malicious intent, thereby attempting to stop abuse before it even starts. Additionally, the field is witnessing a transformative shift in analysing abuse report evidence through the adoption of Large Language Models (LLMs), such as generative pre-trained transformers (GPTs). These models are highly adept at parsing and understanding complex data patterns that could be missed by human investigators, enhancing the efficiency and automation of DNS abuse mitigation efforts, and forming a more dynamic defence against cyber threats. However, this progress also highlights an emerging challenge: the potential for malicious entities to exploit AI technologies themselves ?. Consequently, the intersection of AI and machine learning with DNS abuse mitigation not only heralds significant advancements in cybersecurity strategies, but also emphasises the need for vigilance to prevent these technologies from being used for harmful purposes. This pivotal moment in the fight against DNS abuse underscores the need for ongoing innovation and adaptation to effectively secure digital ecosystems.

3.3.1 Role of AI & ML

The introduction of AI and machine learning technologies into DNS abuse mitigation marks the beginning of an innovative era focused on proactive detection and neutralisation of cyber threats ?. This approach facilitates the rapid analysis of large datasets to uncover patterns indicative of malicious intent in DNS queries. For example, machine learning techniques have been highly effective in analysing DNS queries to classify domain names, significantly improving the detection of domains linked to malware ?. Furthermore, the application of neural network models, such as the Extreme Learning Machine (ELM), has achieved accuracy rates above 95% in the identification of malicious domains, demonstrating the predictive power of AI in combating cyber threats ?. Additionally, the technique of DNS graph mining has illuminated AI's potential within cybersecurity frameworks, with methodologies like belief propagation algorithms achieving high precision in identifying infected hosts and malicious domains. These examples underscore the vital role of AI and machine learning in supporting DNS abuse, paving new avenues for early detection and swift mitigation of potential abuses. However, the complexity of AI models and the demand for transparency in their decision-making processes present ongoing challenges. Integrating AI into DNS abuse mitigation strategies improves security measures, but also requires careful

attention to ethical considerations and the establishment of governance frameworks ?. AI and machine learning can help improve DNS abuse mitigation, but experts must be clear about the problem. It is important to understand how AI models make certain decisions. This helps build trust and ensures that people are responsible for them. There are difficulties in making things clear, such as needing to write down what data was used for training, telling others about the things that affect choices, and explaining how models change to face new risks. It is still difficult to find the right balance between the complexity needed for good threat detection and the openness needed for blame.

In summary, AI and ML are valuable in protecting against rapidly evolving cyber threats and a wide range of devices, including those in the IoT. However, their predictive accuracy can be limited by the quality and quantity of data used for training. Sophisticated attacks designed to evade detection algorithms present a notable challenge, underscoring the importance of continuous learning and adaptation in AI/ML models to maintain their effectiveness.

3.4 Case Studies and Real-World Applications

In recent years, technology has become so widespread that we have witnessed an unmatched number and complexity of cyber threats. A significant vulnerability that can be exploited is the DNS domain name system, a critical part of the internet infrastructure that translates human-readable names into IP addresses ?.

1. Case Study 1: OilRig DNS Tunneling Attack

The case of OilRig reflects the use of custom DNS tunnelling protocols for command and control (C2) operations, thus making it dual-use in nature, both in normal operation and on a fallback communication channel ?. The xHunt campaign ? followed a similar trend of including Snugy backdoor implants in targets of Middle Eastern government organisations and keeping track of them using DNS tunnelling for communication with its C2. These are examples that underscore the strategic use by adversaries of DNS tunneling techniques for stealthiness and resilience within the context of their operations ?.

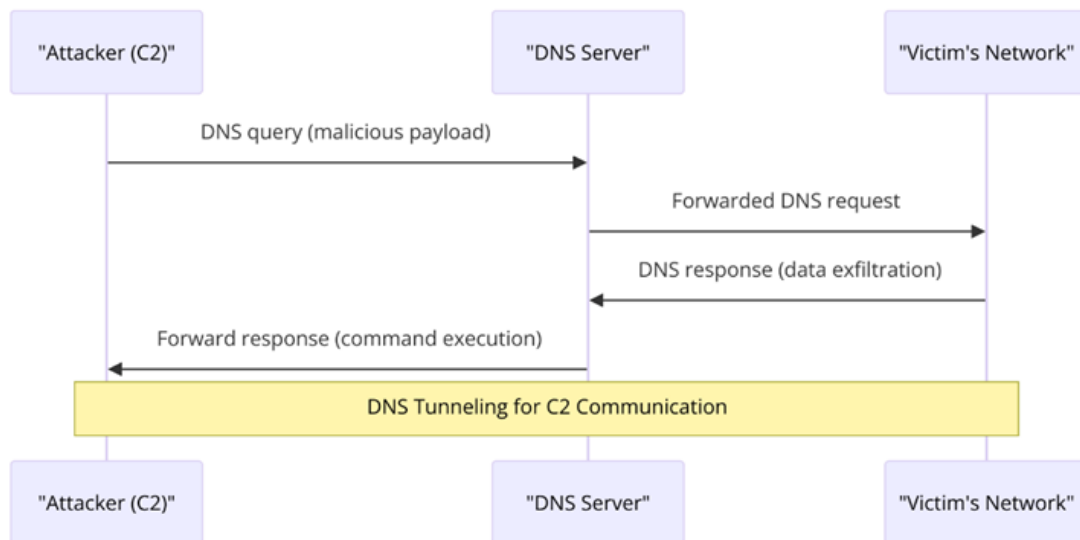


Figure 3.2: DNS tunneling communication between the attacker's command and control (C2) infrastructure and the victim's network.

2. Case Study 2: SUNBURST Use of DGAs

SUNBURST backdoor associated with the breach of the SolarWinds supply chain represents a case in which the use of DGAs is critical, if not only, to conceal communications and system details ?. The SUNBURST backdoor applies the deep use of DNS manipulation for evasion purposes and subsequent attack stages by encoding basic system identifiers and the usage of DGAs for C2 check-ins ?.

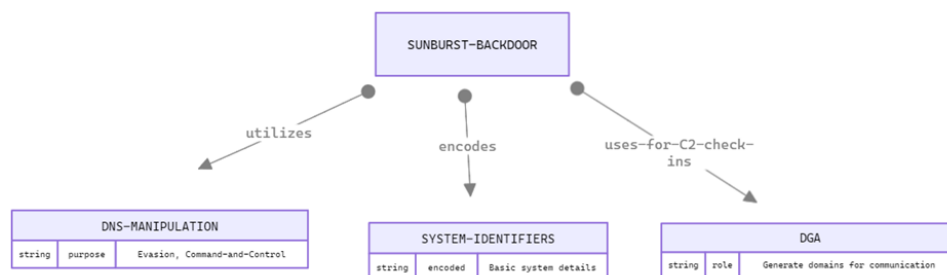


Figure 3.3: SUNBURST backdoor's utilization of DGAs and its associated components.

- Case Study 3: Fast Flux Techniques** The presence of several C2 domains related to the Smoke Loader malware family using Fast Flux techniques only further underscores the difficulties associated with the tracking and eradication of DNS-enabled threats. ?.The major takeaway in the rapid rotation of IP addresses of this method points to the dynamism of strategies used in malicious communications, thus improving the means of defence by cybersecurity ?.

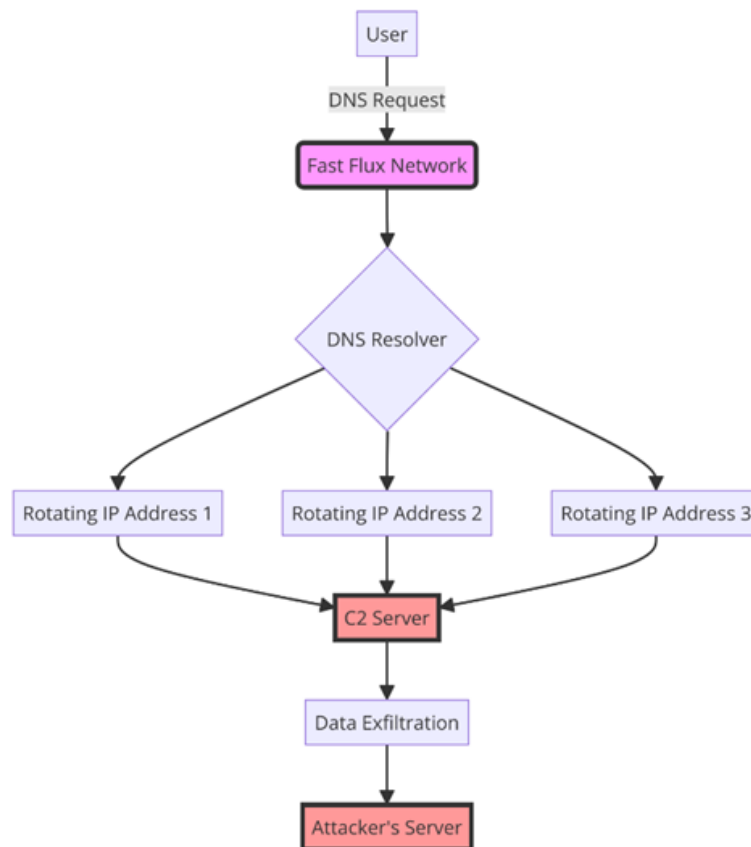


Figure 3.4: The usage of Fast Flux techniques by the Smoke Loader malware family for dynamic C2 domain communications.

4. Case Study 4: Malicious Newly Registered Domains (NRDs)

Malicious NRDs crafted opportunistically in the context of the pandemic expose how threat actors exploit current events to engineer targeted attacks. ? From domains that mirror the information resources of COVID-19 to those that feign government relief programmes, the evolution of such attacks reflects a calculated approach to exploiting public interest and vulnerabilities ? .

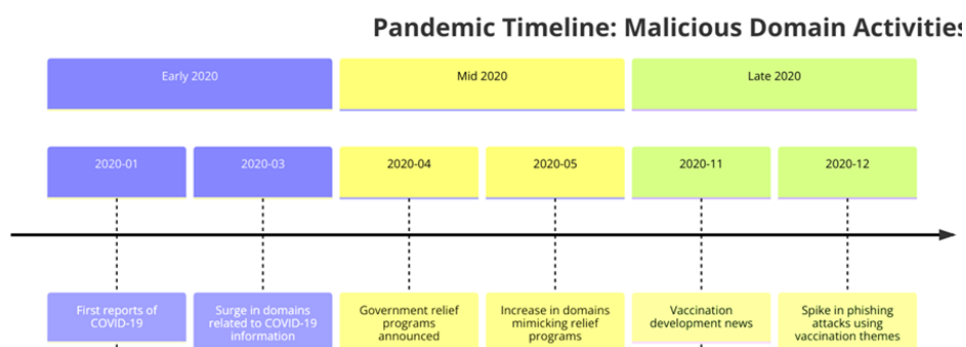


Figure 3.5: The usage of Fast Flux techniques by the Smoke Loader malware family for dynamic C2 domain communications.

In the coronavirus pandemic, too, phishing attacks changed to initially targeting PPE and testing kits, then turning to government stimulus programmes and subsequently enlisting vaccine distribution. Several of them, in fact, employed sophisticated tools, such as MFA pretending as the US Federal Trade Commission and brands such as Pfizer and BioNTech, to steal credentials. where it emphasised that there was a 530% surge in vaccine-related phishing attempts and a 189% increase in attacks on pharmacies and hospitals from December last year to February this year. Advice was given to individuals and organisations that includes being cautious in email and website transactions, advancing security awareness training, and adopting multifactor authentication.

Since January 2020, a total of 69,950 COVID-19 related phishing URLs have been received, of which 33,447 are specifically dedicated to COVID-19. The data have been normalised in such a way that the peak of each topic is at 100%. The results showed much steadier phishing when it came to topics such as pharmaceuticals and virtual meeting platforms (e.g., Zoom) with vaccines and testing showing sharper rises and falls in the attention of scammers.

COVID-Related Topics in Phishing URLs

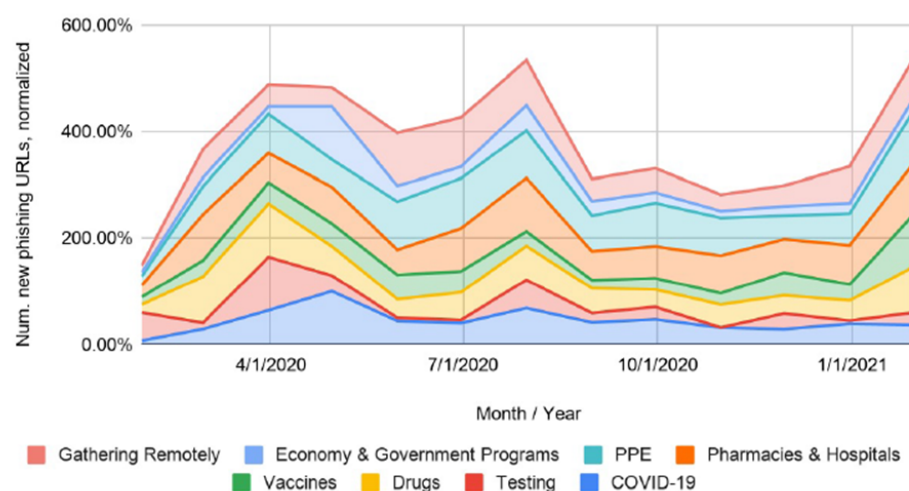


Figure 3.6: Development trends in the majority of COVID-19-related phishing content hosting sites during the period from January 2020 to February 2021. Adapted from ?.

It is evident that a large portion of COVID-19 themed phishing pages targeted leading brands for phishing business credentials, such as Microsoft login, Webmail, and Outlook login. For example, about 23% of these phishing URLs were posed as Microsoft login pages. This threat has particularly highlighted the shift towards remote work in the pandemic, and hence magnified the relevance of these attacks as one of the foremost methods that bad actors are taking on.

Popular Phishing Targets in COVID-Related URLs

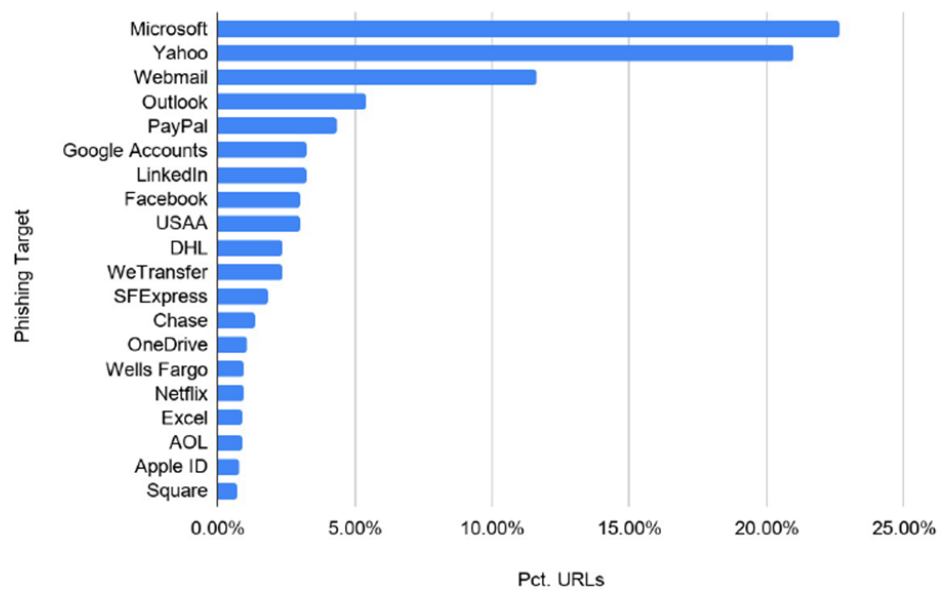


Figure 3.7: Top spoofed websites in COVID-themed phishing attacks (global), where the percentage in each column is the percentage of phishing volume per site and category. Adapted from ?.

Thus, this clearly indicates a situation whereby the attackers set up websites frequently for COVID-19 themed phishing attacks. Many of these phishing pages are found on sites created less than 32 days, meaning that these sites are launched with specific purposes in view of these imminent attacks. The strategy allows attackers to customise their messages and URLs to the current pandemic trends, indicating the dynamism behind such cyber threats.

Website Age (at Detection Time) for COVID-Related Phishing URLs

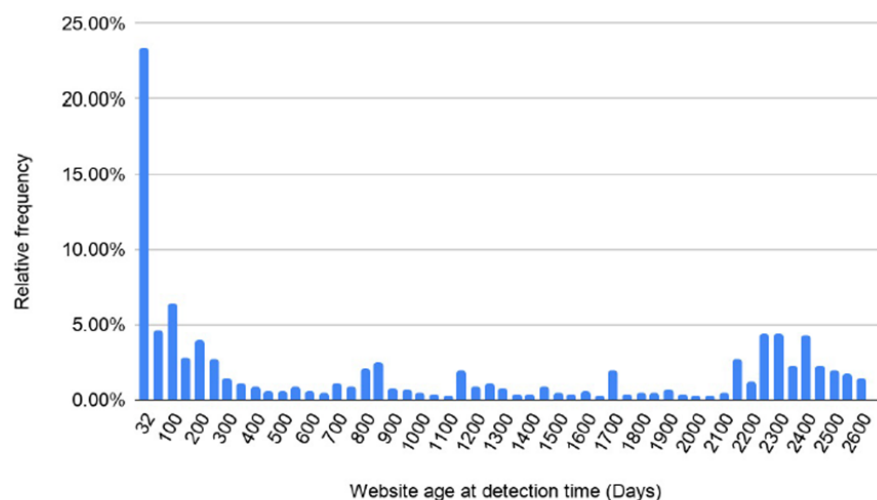


Figure 3.8: Statistic of lifespan distribution of COVID-19-related phishing content hosting sites when the sites are reported. Adapted from ?.

3.5 Challenges & Future Directions

Mitigating DNS abuse demands an immediate stop to the rapid evolution of cyber threats, underscoring the critical need for rapid global cooperation and the implementation of advanced technology. The key challenge is to achieve a fine balance between reducing false positives and accurately identifying genuine threats, while simultaneously advancing beyond the limitations of outdated technologies ?. The future of this domain largely depends on researchers' ability to enhance technological solutions, particularly focussing on the improvement of AI algorithms for deeper analysis of DNS traffic patterns. This opens a promising pathway for the creation and application of locally developed tools, providing innovative strategies to strengthen DNS defences. The ability to navigate the complex landscape of DNS abuse will require stakeholders to be agile in responding to emerging threats and developing novel solutions. The collective push towards the evolution of technology and methodologies will play a pivotal role in shaping effective DNS abuse management strategies in the years ahead.

3.5.1 Identification of Current Challenges

Mitigating DNS abuse involves developing strategies that should not only be proactive, but kept constantly up to date to handle the changing environment of cyber threats. The fluid nature of these threats means updating current protocols as well as developing new defence methods. With bad actors constantly reviewing their methods to take advantage of the vulnerability of DNS, it has become imperative that the cybersecurity industry continuously updates its defence mechanisms ?. Being a global phenomenon, the Internet and hence DNS abuse being transnational in character, there is no other alternative than international cooperation. The effectiveness of DNS abuse management would be based on collaborative work across national borders, where experts in different geographical areas come together to share their knowledge and resources ?. The legal and regulatory framework varies in the various jurisdictions, making it difficult to reach a consensus on the regulations, standards, and enforcement actions. Another big challenge is that, to mitigate DNS abuse, the requirement is necessary to eliminate both false positives and negatives. Balance must be established in such a way that rather strict measures may reduce user experience, while, at the same time, being liberal might bring less detection of malicious activities. The cybersecurity community must continue to advance its detection and response capabilities, due to the increasing levels of sophistication used by DNS abusers. This will keep the security and integrity of the DNS system in good shape, thus protecting this vital part of the Internet infrastructure.

3.5.2 Discussion on Future Research Directions and Technologies

At the ICANN77 meeting, developments on mitigating DNS abuse were presented. These included the draughting of changes mandating that registrars and registries respond to abuse notifications, which contributed to a decline in global abuse levels after Freenom's legal response. Although the ccNSO Domain Abuse Steering Committee argued for a proactive mitigation strategy, the gNSO's analysis found minimal abuse rates in EU ccTLDs, which it attributed to market maturity and non-profit models ?. To improve domain security and enable international cooperation against changing cyberthreats, future initiatives will focus on creating cutting-edge tools and using technologies such as artificial intelligence and machine learning. This means that we need to look at more complex AI and machine learning tools that can understand the details of web traffic, which will make the results more accurate and stop the sending of wrong signals ?.

3.6 Summary of Findings

Research on the transparency of DNS abuse mitigation emphasises how threats are always changing and how mitigation techniques must evolve as well. It highlights how important community involvement and transparency are to fostering trust. Although technological advancements, especially in AI and machine learning, are essential for threat detection, their implementation must be carefully considered. Practical examples provide insight into the efficacy of various strategies. Maintaining a balance between new mitigation measures and effective teamwork and communication is a constant issue. To effectively address DNS abuse, future efforts should focus on using technology, international cooperation, and standardised information exchange.

4 Research Methodology

A structured questionnaire was sent by email to various stakeholders in the DNS ecosystem. This method was chosen because of its convenience, compliance with participants' busy schedules, and permission for detailed responses at the respondents' will. The approach provided a means of soliciting a wide range of expert observations on DNS abuse in terms of definition, the most prevalent types, mitigation challenges, and the theme of transparency.

4.1 Questionnaire Design and Distribution

The questionnaire had to take into account all of these issues in a multidimensional approach, giving great emphasis, but not limited, to address the nature of DNS abuse mitigation transparency.

The questions were specifically designed to extract in-depth information about:

1. The definition of DNS abuse.
2. The types of DNS abuse stakeholders most commonly encounter, aiming to identify prevalent patterns and specific concerns within the ecosystem.
3. The challenges and limitations faced in mitigating DNS abuse, seeking to understand the barriers to effective action.
4. The mitigation strategies used, gathering information on the practical steps taken and their perceived effectiveness.
5. The practice of publishing reports or data as a form of transparency, exploring the current state of openness in the field.
6. The role of transparency in aiding or impeding DNS abuse mitigation efforts, probing the potential impacts of increased visibility.
7. The effects of transparency on the relationships between various DNS stakeholders, considering the broader implications for cooperation and trust.

4.2 Stakeholder Responses

The insights from the completed questionnaire of the different stakeholders reflect several key themes and insights critical to understanding DNS abuse, as well as the mitigation of this abuse. These include various perspectives on what exactly the definition of DNS abuse is, the types of abuse most observed, and the difficulties experienced by stakeholders in efforts to mitigate its abuse. Additional discussions are related to mitigation methods, which provide a full view of current practices and potential areas for improvement with respect to the DNS ecosystem.

Key themes and insights :

- **Varied Definitions of DNS Abuse:** Although stakeholders largely accepted the definition that had been adopted by the ICANN Contract Parties, they also noted its shortcomings, especially in being too categorical and thus may leave out evolving types of abuse. It was considered that a more flexible way forward would be a robust framework to define the abuses to be mitigated at the domain name level.
- **Common Types of DNS Abuse:** They pointed out that phishing was the most common attack type, followed by malware, botnets, and spam. It was also pointed out that one of the most common problems was related to the challenge related to proving the number of spam-related domains.
- **Challenges in Mitigation:** Perhaps the most significant was the economic structure of the domain registration industry, its ability to mitigate malicious registrations without fundamentally altering it. Stakeholders clearly state that a significant difference between large registrars, generally considered good actors on the Internet, and smaller registrars with a higher level of DNS abuse underscores the different aspects of this problem within different industry segments.
- **Mitigation Strategies:** The responses included different strategies, such as blocking orders from some regions or using software to monitor abusive activities. Recommendations were made on the role of education and outreach, including relevant projects such as NetBeacon and Compass to report abuse and information on DNS abuse.
- **Role of Transparency:** Opinions on transparency were mixed since part of the respondents consider this positively because it is a tool that provides evidence to the industry in its fight against abuse, part of them consider it negatively as sensitive mitigation ways could be revealed. The impact of transparency was also elaborated on developments in relationships between all stakeholders, and there is in general agreement that transparency will increase understanding and teamwork through better

communication on measures set against abuse.

The responses of the stakeholders significantly enriched the research by providing a detailed look at the practical challenges and strategies to mitigate DNS abuse. The responses not only offered valuable real-world perspectives, but also highlighted the importance of adaptive definitions, comprehensive mitigation strategies, and thoughtful consideration of transparency's role in the ecosystem. This analysis bridges theoretical knowledge with the experiences of those actively involved in mitigating DNS abuse.

4.3 Types of DNS Abuse Encountered

The stakeholder responses provided details of the most prevalent forms of DNS abuse that were being encountered within their specific ecosystem. These insights reveal a view of the various types of abuse, each of which poses unique challenges that require tailored mitigation strategies.

1. **Phishing:** Stakeholders identified it as the most prevalent form of DNS abuse and the most visible. In fact, the total number of phishing incidents observed through tools such as NetBeacon and tracked by Compass is a stark and singular metric of just how big and urgent the problem has become in the wider DNS domain.
2. **Malware and Botnets:** These also included malware and botnets, i.e. multifaceted DNS abuses. Such abuses not only compromise the integrity of systems but also present a security hazard to users and infrastructures in general.
3. **Spam:** It is now recognised as widespread, and stakeholders have pointed out the challenges of quantifying and appropriately addressing the relevant spam-related domains. Therefore, it makes spam elusive for existing mitigation efforts that raise the bar with respect to the pursuit of next-generation detection and response mechanisms.
4. **Compromised CMS :** Encounters with compromised content management systems (CMSs) have been referred to as common encounters. Consequently, such attacks are possible in cases of some other existing vulnerabilities in web platforms. This kind of abuse reinforces the need for strong web security control practices and the need for vigilance among platform operators.
5. **"Water Torture" Attacks:** Known as random subdomain attacks, they represent a more technical and sophisticated form of DNS abuse. These attacks not only disrupt normal DNS operations but also require advanced countermeasures to effectively mitigate their impact.

The varied nature of DNS abuse that stakeholders encounter underscores the fact that community efforts must continue to build on ongoing collaboration, innovation, and

education to address these challenges effectively. This is derived from the experiences of stakeholders and forms a basis of paramount importance on which effective strategies and policies will be formulated in the mitigation of DNS abuse.

4.4 Challenges in Mitigation and Mitigation Strategies

The responses of stakeholders demonstrated details of the multifaceted challenges in mitigating DNS abuse, coupled with the various strategies used to address these issues.

1. **Economic and Technical Hurdles:** A significant barrier identified was the economic structure of the DNS industry, characterised by low margins and high volumes, often limiting the resources available for robust mitigation efforts against DNS abuse. Stakeholders highlighted that about 80% of malicious domain registrations could be traced back to a mix of large, well-known registrars and smaller entities with disproportionately high levels of abuse. This economic reality complicates the implementation of effective mitigation strategies, underscoring the need for innovative solutions that are both cost-effective and scalable.
2. **Regulatory Gaps:** The regulatory environment was also cited as a challenge, including poor, weak, or absent policies and enforcement mechanisms that could not effectively handle DNS abuse effectively. Stakeholders pointed out the necessity for clearer regulations and standards that can guide the industry's anti-abuse efforts more effectively.
3. **Mitigation Strategies:** Stakeholders have responded to this with a variety of mitigation strategies. They placed an emphasis on components of education, collaboration, and outreach to raise awareness and develop a social response to DNS abuse. Technological solutions such as abuse reporting intermediaries (NetBeacon) and measurement projects (Compass) that measure the Internet are vital in finding, reporting, and understanding abuse cases. Designed to improve reporting and mitigation, these tools can also capture essential data with a character that helps inform policy and regulatory responses.

4.5 Transparency in DNS Abuse Mitigation

The responses of stakeholders underscore the subtle perspective on transparency within the DNS abuse mitigation framework, highlighting both its potential benefits and challenges.

1. **Benefits of Transparency:** Increased transparency is widely recognised as a way to demonstrate commitment in the industry to defend against DNS abuse. It will

encourage normalisation of mitigation efforts throughout the ecosystem, which means that proactive activity becomes more commonly adopted and attributed to a culture of responsibility and accountability. Transparency in reporting abuse metrics and mitigation outcomes can also enhance trust between users, regulators, and within the industry itself, promoting a unified approach to addressing DNS abuse. In addition, transparency is seen as a contributing element in improving understanding and cooperation among various entities involved in the DNS, including operators, registrars, registries, and regulators. By sharing information on abuse trends and mitigation strategies, stakeholders can better appreciate each other's challenges and contributions, leading to more effective collaborative efforts.

2. **Challenges and Concerns:** Stakeholders raised several concerns about the degree and manner of transparency. One point of concern is that some sensitive mitigation strategies could be exposed that, in turn, could serve as a support for malicious actors, allowing them to discover ways to detect and mitigate abuse. This fine balance between providing useful information and protecting operational integrity is a significant challenge for many in the industry. Furthermore, there is apprehension that increased transparency might lead to regulatory or legal consequences, especially if disclosures are mandated in a manner that does not consider the practical aspects of abuse mitigation. The stakeholders also mentioned operational challenges, such as the capacity to complete transparency reporting, given the current reliance on less formal mechanisms for reporting abuse and monitoring mitigation.
3. **Strategic Approach to Transparency:** Stakeholders advocate for a strategic approach to transparency that supports the goals of mitigation of DNS abuse without compromising the effectiveness of these efforts. This includes targeted transparency that focuses on aggregate data and trends rather than detailed disclosures of specific mitigation actions or techniques. Additionally, fostering an environment where sharing information does not lead to punitive outcomes, but rather supports collaborative improvement, is considered essential. Although the value of transparency for the mitigation of DNS abuse is considered high, stakeholders cautiously advocate that every step be done with care with regard to what, how, and to whom it shall be disclosed. A balanced approach that improves the collective ability to address DNS abuse while safeguarding the methods used is crucial for the ongoing evolution of transparency practices in the industry.

4.6 Impact on Relationships within the DNS Ecosystem

Stakeholders pointed to a clearer potential impact on meaningful relationship building within their particular DNS ecosystems: greater transparency and mitigation. Better transparency

is seen by creating a better understanding among different parties, for instance, among registries, registrars, and regulators about challenges and works against abuse, hence their collaboration and trust that improves combined efforts against abuse. However, this provision raises concerns that such transparency could get to the point of obstructing informal cooperation in general or actually reveal sensitive techniques from an operational standpoint detrimental to entities working together. Balance is a key element to ensure that these issues are addressed and that partners work harmoniously with each other within the DNS community.

4.7 Analysis and Data

The detached examination of stakeholders' emailed responses in regards to DNS abuse and its various connotations is reported herein. In relation to those themes, the following record the main important points.

Definition Supported	Comments and Suggestions
ICANN Contracted Parties' Definition	Endorses the ICANN definition for its clarity and actionability. However, it suggests that it may be too narrow and advocates a more flexible framework to encompass evolving threats. Points to a self-authored sophisticated way of defining harms at the domain name layer, promoting adaptability.
Critique of ICANNwiki Definition	Finds the ICANNwiki reference lacking, preferring the SSAC 115 report definition for its broader applicability and recent adoption in RAA amendments.
Mixed Views	While there's alignment with the existing categorical definitions for practical reasons, there is a shared belief in the necessity for definitions that evolve with emerging DNS threats. The discussion indicates a desire for a balance between categorical clarity and adaptability to new forms of abuse.

Table 4.1: Varied Definitions and Understandings of DNS Abuse

Type of DNS Abuse	Frequency Mentioned	Stakeholder Comments
Phishing	Most Common	Identified as the primary concern across responses, significant impact observed.
Compromised CMS and Confusable Domains	Frequently Mentioned	Highlighted as a prevalent issue alongside phishing and other platform abuses.

Table 4.2: Types of DNS Abuse Encountered

Challenge Type	Stakeholder Insights	Suggested Solutions
Economic	High volume, low margin business model impedes anti-abuse efforts.	Calls for industry-wide collaboration and support.
Regulatory Gaps	Lack of clear regulations complicates mitigation efforts.	Advocates for establishing and following industry-wide best practices.

Table 4.3: Challenges in Mitigating DNS Abuse

Strategy	Description	Stakeholder Feedback
Blocking Orders	From certain regions to mitigate abuse.	Implemented alongside other criteria to make services less appealing to abusers.
Education & Collaboration	Outreach to improve awareness and cooperation.	Viewed as essential, with a need for more systematic implementation.

Table 4.4: Mitigation Strategies Employed

Aspect of Transparency	Benefits	Concerns
Reporting Abuse Metrics	Enhances trust and accountability in the ecosystem.	Risk of exposing sensitive mitigation techniques if not managed carefully.

Table 4.5: Transparency in DNS Abuse Mitigation

Relationship Aspect	Positive Impacts	Potential Challenges
Between Entities	Improved understanding and collaboration from shared data.	Concerns about competitive sensitivity and operational integrity could limit openness.

Table 4.6: Impact on Relationships within the DNS Ecosystem

In analysing the data from the stakeholder responses, a thorough examination of DNS abuse has been carried out. The stakeholders, deeply embedded in the DNS ecosystem, provide valuable information on the definitions and manifestations of DNS abuse. They highlight phishing as the most common and worrying type, with compromised CMS and confusable domains also noted for their prevalence. Challenges in mitigation are primarily related to economic factors and regulatory gaps, where the structure of the industry alters mitigation abuse actions and the lack of clear regulations muddy the waters. Mitigation strategies like targeted blocking and collaborative education are in play, though their implementation faces

hurdles due to the industry's focus on throughput and the capacities of various entities. The role of transparency is acknowledged as double-edged; although it could foster accountability and trust, there is a risk that bad actors exploit sensitive techniques. Stakeholder experiences and strategies contribute to a deeper understanding of DNS abuse, suggesting the need for a multifaceted approach that involves adaptation, collaboration, and a careful balance of transparency.

5 Implementation

This chapter focuses on practical implementation with respect to the Domain Legitimacy Checker. The multiviewed approach, along with programming in Python and the web framework in Flask, HTML, CSS, JavaScript, on the side of external APIs, assisted greatly in making a resilient framework for DNS abuse detection and transparency improvement. With these alternatives, I came up with this simple but effective way not just of finding legitimacy in domain names, but also of showing plainly and clearly the various tactics with which bad actors are using in the adoption of confusable domains for phishing and malware distribution, along with other malicious activities to help me with my research. This endeavour embarked on a journey from the idea to execution, focusing on a user-friendly web interface that allows users to quickly identify potentially malicious domains.

5.1 System Overview

The development of Domain Legitimacy Checker was chosen because the system is such a robust web-based platform that is tasked with the identification and analysis of domain names that can be malicious. The user first initiates domain name requests through the user interface. This request is processed by the Flask-based web server that orchestrates the core operations of the system. Domain Analysis Engine is meant to perform an analysis on DNS abuse patterns exhibited by the submitted domain using heuristics and pattern matching algorithms. For a deep check, the system queries external APIs such as VirusTotal for additional checks of legitimacy. The results of such checking are kept in a database as well, which gives out the history of known malicious domains. Finally, the Results Display component gives control of the results back to the user. Figure 5.1 provides an illustrative view of the architecture of the software system design and the information flow.

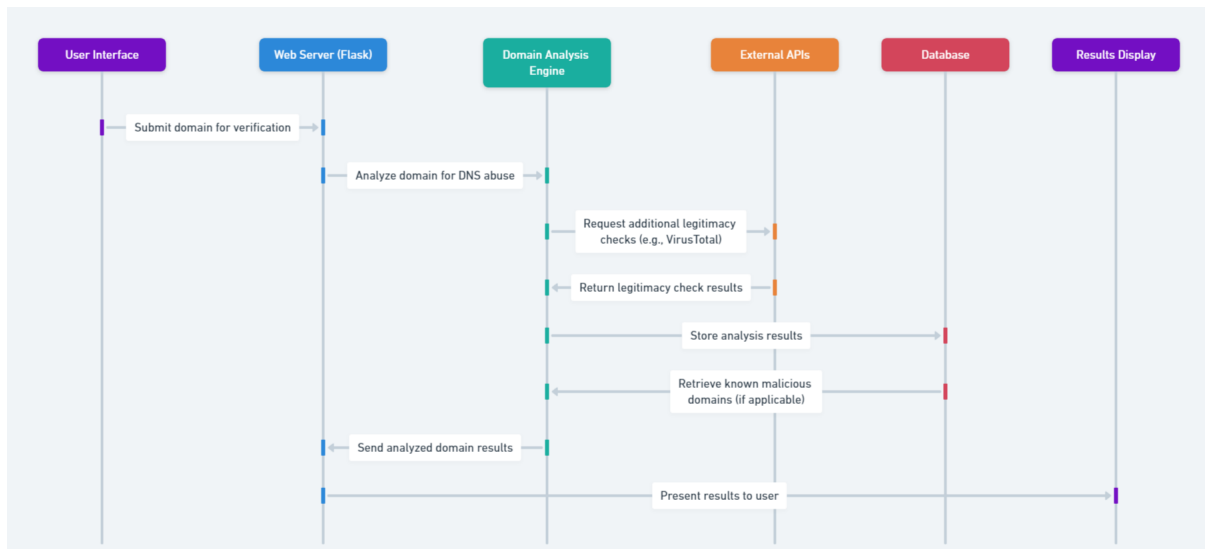


Figure 5.1: Domain Legitimacy Checker

5.2 Integration

5.2.1 Backend Implementation

The server side : Python on the Flask framework was used for implementing this side. The server works better with a solid web server in case you are time pressed because the learning curve on Flask to make it implement is not that steep. The Flask application is set to work through a series of endpoints, each of which corresponds to a set of functionalities with respect to the system, among which is an endpoint for submitting domains to ascertain the results of their analysis. A request comes into the Flask server, and for any incoming given request, it simply calls the indicated function to handle the process relevant to the request: a process to parse the input data, to start domain checks, or to respond with the check results.

API & library : The Domain Analysis Engine forms the main core within the backend, responsible for DNS abuse detection. This is realised by creating some of the changes that the submitted forms of domain names have so that possibly malicious or confusable counterparts are recognised with the assistance of pattern recognition algorithms. In addition, the development leverages libraries and packages such as "dnspython" and requests to conduct the queries to DNS and "request" APIs with respective libraries. This system communicates with external APIs such as "VirusTotal" in order to perform legitimacy checks, whereby the fact is made up for carrying out thorough analysis and reliable detection of malicious domains.

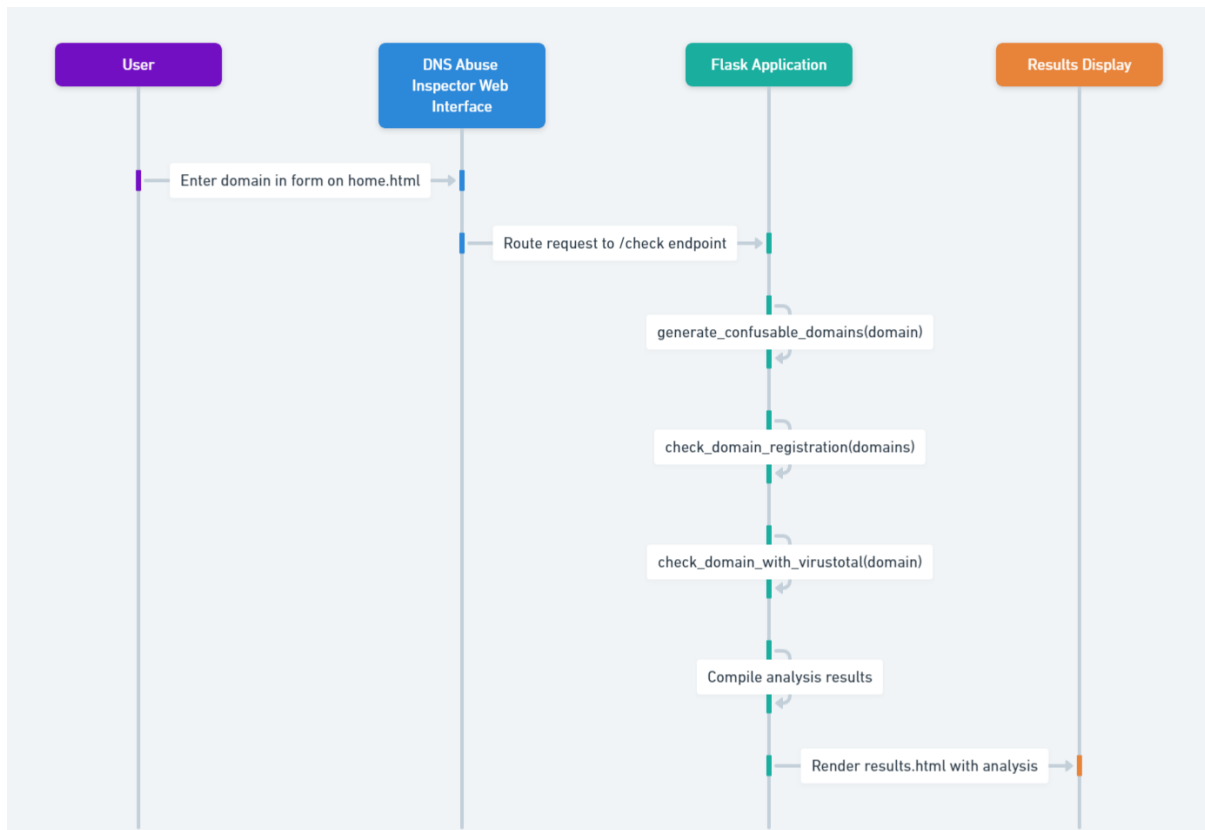


Figure 5.2: Domain Legitimacy Checker System Interaction Workflow

5.2.2 Frontend Implementation

Web Interface: HTML was used and then styled with CSS, and fine-tuned with Bootstrap, the user interface has responsiveness built in and is very user-friendly for use, regardless of the device that it is being used on. The interface is user-friendly, from submission of the initial domains easily, to displaying results, intending an automatically flowing process designed simple for the layman.

Interactive elements: JavaScript is used to bring in interactivity to most of the pages bringing the interactivity to the web app domain submission pages. These respect real-time, giving feedback even for the submission of domains, for instance, changing the text of the submission button to "Analysing." and avoiding its swarming with submissions. These dynamic elements in the front-end make the process of domain analysis even more visually responsive, which increases users' engagements and trust in how the system processes.

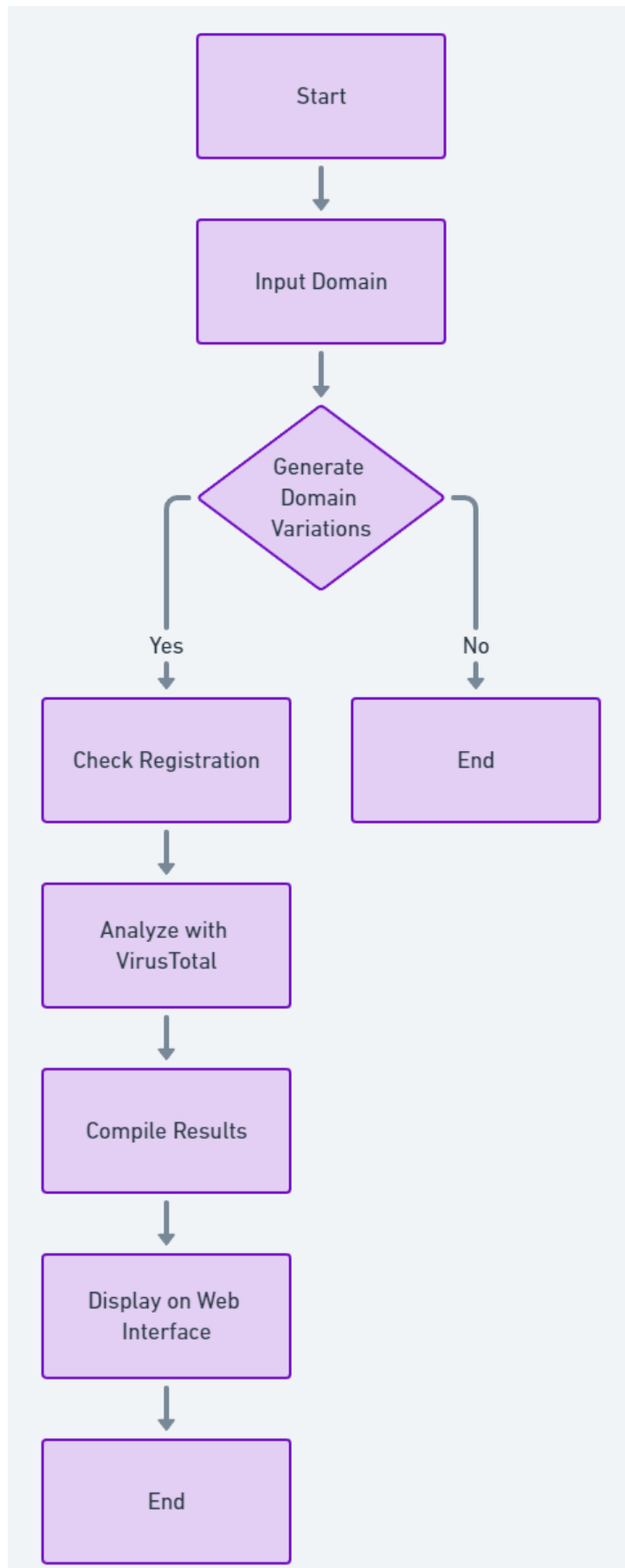


Figure 5.3: Domain Legitimacy Checker

5.3 Tools & Technologies

Domain Legitimacy Checker was built using Python with the usage of its third-party modules for development and to provide ways for integration with systems. The platform was powered by Flask, which is a framework that serves requests using the HTTP protocol. The front-end is developed using HTML5 in the structuring of web content and empowered by CSS3 for styling, while allowing Bootstrap for responsive design for all devices. JavaScript provides web pages with simple, interactive, and dynamic functionality. It has also used libraries such as dnspython for the support of DNS queries, which are key in the lookup of domain registration. The request libraries also connect to external APIs like VirusTotal for the legitimacy analysis of a domain.

It takes advantage of the scanning powers of VirusTotal API, which has several security engines and site scanners to indicate how safe a domain is. It derives its value from domain security, in contrast to the domain name, with thousands of sources and other indicators. Importantly, domains that are already blacklisted for hosting phishing sites, distributing malware, or participating in suspicious activity should be filtered. The choice of each of the tools and technology used was based on its individual merit, but by their integration, making sure that all the systems combined to achieve the cohesiveness and effectiveness of detecting DNS abuse and transparency.

5.4 Visualisations

The interface and layout of the web page have been designed for ease and smooth transition with users. The interface was specially designed by which our users can easily verify whether the domain is legitimate. As with all its applications. Upon loading, the domain legitimacy checker presents itself with a very neat and simple layout. The hero section comes with the name of the application. The domain name input field is at the heart of the page, which requires the user to type the domain url they wish to analyse. Once a domain is submitted, the system springs into action, processing the input through various checks and analyses. The server logs these interactions, as seen in subsequent visualisations, ensuring that every step of the process is recorded for performance monitoring and optimisation.

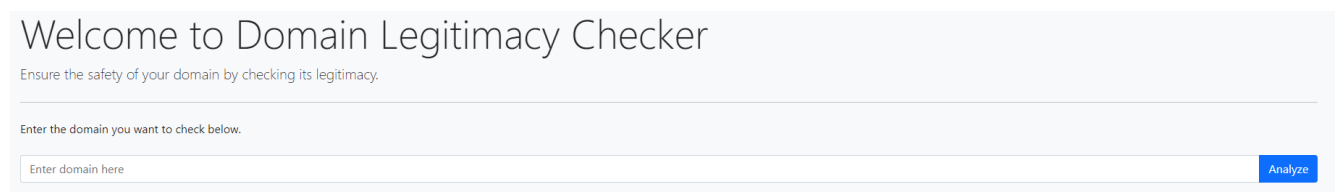
The image shows the main interface of the Domain Legitimacy Checker. At the top, there is a heading "Welcome to Domain Legitimacy Checker" in a large, dark font. Below it, a smaller subtitle reads "Ensure the safety of your domain by checking its legitimacy." A horizontal line separates this header from the main content area. Below the line, there is a prompt "Enter the domain you want to check below." followed by a text input field with the placeholder text "Enter domain here". To the right of the input field is a blue button with the text "Analyze" in white.

Figure 5.4: The main interface of the Domain Legitimacy Checker

5.4.1 Input & Interaction

The Domain Legitimacy Checker Tool provides an intuitive place for interaction with users to ensure a seamless experience. The domain input method, a single-field form intended for simplicity of use and quick analysis, is at the centre of this interaction.

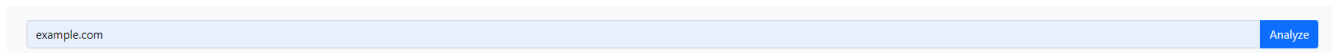


Figure 5.5: The domain input box where users begin their interaction with the Domain Legitimacy Checker.

First, the user is asked to enter a domain of their choice and to put it in a text box, minimally styled to not distract but to point the user's focus in performing the task. Right next to the text box is the "Analyze" button, contrasting with blue to stand out visually and identified for the user as the next step to take in the process. This design invites immediate action upon domain entry, providing a clear path from user input to results.

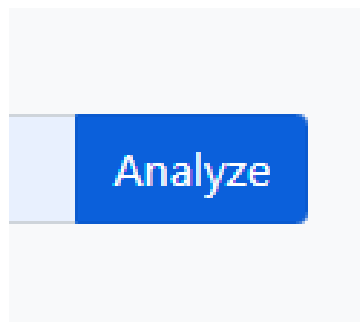


Figure 5.6: The 'Analyze' button, poised for user action after domain entry.

The user's request to check a domain is initiated as soon as a domain is entered into the 'Analyze' field and the button is hit: a series of background checks are run to understand the eligibility of the domain. It is at this point with the changing request of the user that his request is no longer an action but a graph analysis that is being done by the systems running in the back end.

5.4.2 Interactive Features

The programme comes with an interactive interface; the user is engaged in all the steps from entering a domain for analysis to receiving the results. In fact, starting from the second users have done submitting a domain for analysis, this very step will start a circle of HTTP-requests, which the server logs with great care. These logs are dynamic, real-time visualisations of user-server interaction rather than just recordings.

The moment a 'click' on the 'Analyze' button happens, the server instantly receives a 'POST' request through the endpoint '/check', which notes that the action marks the start

of the domain analysis. On a successful request, a '200' status code is returned to signify a successful search. Such types of interaction go down as entries into the server log, forming a very critical and highly detailed timeline of activities.

```
127.0.0.1 - - [13/Mar/2024 14:15:48] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [13/Mar/2024 14:15:48] "GET /static/style.css HTTP/1.1" 404 -
127.0.0.1 - - [13/Mar/2024 14:16:07] "POST /check HTTP/1.1" 200 -
127.0.0.1 - - [13/Mar/2024 14:16:11] "POST /check HTTP/1.1" 200 -
127.0.0.1 - - [13/Mar/2024 14:16:11] "GET /static/styles.css HTTP/1.1" 404 -
```

Figure 5.7: Server log entries capturing real-time HTTP requests and responses

If there is any issue, these logs are highly important, for example, in the case of "404 - Not Found" error in the requested resource. They not only instantly inform system administrators what might have gone wrong, but also act as hints for such troubleshooting. Log analysis allows an administrator to automatically correct problems.

5.4.3 Results Display

The Domain Legitimacy Checker displays the findings in an easy-to-understand style after the completion of the domain legitimacy research. Every domain has an icon next to it; an exclamation point indicates that the domain is possibly harmful and a checkmark indicates that the domain is not malicious. The initial level of result interpretation is this visual feedback, which enables users to assess domain safety rapidly. "365.com and paypal.com" were tested in 5.8 and clearly show how the programme works when domain names are inserted.

Domain	Malicious Status	Detection Details
365online.co	Malicious: No	
365online.com	Malicious: Yes	<ul style="list-style-type: none"> Detected by Seclookup: malicious Detected by Segasec: phishing Detected by Webroot: malicious
3650online.com	Malicious: No	
365online.com	Malicious: No	
36online.com	Malicious: No	
35online.com	Malicious: No	
65online.com	Malicious: No	
paypal.com	Malicious: Yes	<ul style="list-style-type: none"> Detected by BitDefender: malware Detected by CyRadar: malicious Detected by Fortinet: phishing Detected by G-Data: malware Detected by Lionix: malicious Detected by Seclookup: malicious Detected by Sophos: phishing Detected by VIPRE: phishing Detected by Webroot: malicious
paypal.com	Malicious: No	
payppal.com	Malicious: Yes	<ul style="list-style-type: none"> Detected by Seclookup: malicious
paypal.co	Malicious: Yes	<ul style="list-style-type: none"> Detected by BitDefender: phishing Detected by CyRadar: malicious Detected by Seclookup: malicious Detected by VIPRE: phishing

Figure 5.8: visual indicators showing the legitimacy status of analysed domains.

For domains identified as malicious as you can see above, the interface unfolds additional information, providing a breakdown of the detected security threats. The findings of each scanner are listed below the domain, revealing the specific categories of malicious activity identified, such as malware, phishing, or other security threats. This level of detail is not only informative, but also actionable, guiding users on potential next steps for mitigation or further investigation.

5.4.4 Navigating Results

After the results from the domain check come back, the Domain Legitimacy Checker would allow the user to easily explore more domains that interest them. It normally does this through a button that shows prominently on the interface for this function and that simply says "Check Another Domain." Basically, this reconnects the user with the input interface.

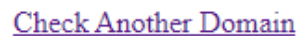


Figure 5.9: The 'Check Another Domain' button

This iterative process is another valuable characteristic of the user journey, so it can be continued non-stop right on the search results page. This squarely builds on the design philosophy of the tool, that of making the user capable of doing as many searches in as lean a manner as possible, fostering an environment of proactive web security.

5.5 Challenges & Solutions

During the development of the Domain Legitimacy Checker, I faced several challenges, each requiring a tailored solution to ensure the project's success.

Challenge 1: API rate limit The frequent use of the VirusTotal API presented a challenge due to its rate-limiting constraints. Exceeding the allotted number of requests would lead to temporary blocking of our service.

Solution: Implement a queuing system with a delay mechanism to spread the requests over time, adhering to the API's rate limits. Additionally, we cached the results of previous queries to minimise repeat requests for the same domains.

Challenge 2: Real-time Feedback for Users, therefore, is very important to give very instant feedback in the process of the domain analysis, but was otherwise very hard to prove because of the asynchronous behaviour, in principle for network operations.

Solution: Using asynchronous JavaScript to send information to the servers and receive results from them without refreshing the web page.

Challenge 3: Handling Malicious Domain Variations Identification and generation of a full set of confusing domain variations represented a key computational challenge.

Solution: Using a combination of common substitution algorithms and a heuristic approach, which prioritised variations based on their likelihood of being used in phishing attacks.

Challenge 4: Data Storage & Retrieval Efficiency Storing analysis results for quick retrieval while managing database performance was a concern, especially with the growth of the data set.

Solution: implementing a real-time domain analysis system with external APIs for comprehensive domain validity checks and creation of algorithmic domain variations to assess potential security risks.

Challenge 5: System Scalability As the system's user base grows, so does the load on our servers, which initially led to concerns about scalability.

Solution: The system was designed with scalability in mind, using Flask's built-in capabilities to handle an increasing number of simultaneous user requests.

By addressing these challenges with careful planning and adaptive solutions, we improve the reliability, performance, and user satisfaction of the system.

5.6 Testing & Validation

The domain legitimacy checker follows rigorous measures in testing the system, which ensures both dependability and accuracy. In the implementation, the back-end logic had a number of things implemented with unit tests; we have used the Python unittest framework. We use mock objects to simulate the acts of external APIs. Manual and automated tests were performed in front-end technologies. Automated UI testings, such as those with Selenium, were relied upon to ensure that all interactive elements are operable. The interface has been tested both automatically and manually, with the help of loading a page on a few browsers and mobile devices to ensure that the interface is responsive and behaves similarly. Continuous Integration (CI) pipelines was set up so that every time a new code commit passes to run tests, ensuring that newly made changes do not break existing functionalities automatically.

6 Evaluation & Discussion

In this chapter, I will focus on evaluating and discussing two forms of DNS abuse, which are confusable domains and phishing due to their popularity among bad actors by testing and validating them. I will dive into real-life examples to illustrate the severity of these threats and examine existing mitigations and techniques used to mitigate them to test how well my project met the objectives. Additionally, I will propose to improve transparency around these mitigation strategies to foster accountability and trust. Through analysis, I will assess the feasibility of implementing such transparency measures by performing an analysis using data and evidence. Finally, I will address the limitations of my work. This comprehensive approach aims to provide information on how to effectively address DNS abuse while promoting transparency in the process.

6.1 Confusable Domains

6.1.1 Identification & Examples of Targeted Domains

The choice of such domains to target and outsource depends on many factors, each with its implications on business strategy, marketing, and law enforcement. The selection of these domains hence matters a lot in creating potential conflict, especially those related to existing trademarks. Understanding these selection criteria is very important in trying to negotiate the hurdles of the digital market and in protecting rights through intellectual property. To navigate these complexities effectively, it is essential to consider several key factors.

- **Commercial Appeal:** The domains with commercial appeal attract traffic and can generate income. They are short and memorable and relate to popular products or services, sometimes leading to ownership arguments ?.
- **Keyword Relevance:** Similarly, a domain specific to keywords ranks well in the search and indirectly lures organic traffic, which will help enormously the business in the search for common search queries and, in this process, generates more clicks.
- **Similarity to Well-known Trademarks:** Domain names, when similar to those of famous trademarks, can cause legal trouble for the trademark owner. laws prevent

confusion and protect the brand reputation in disputes.

6.1.2 Real-life examples

- **Cybersquatting** : registering domain names that closely resemble trademarks or brands and selling them at exorbitant prices; this also includes advertising to earn money, collecting email, or even jumping to evil websites. One such renowned case was that of Amul, a major dairy company in India, during 2019-2020. Amul had an impersonation case of similar domain registration for purposes of phishing, which lured people into fraudulent schemes like fake distributorship or job opportunities. In the last three years, from 2018 to 2020, this issue forced Amul to issue public notices and take legal action against such misuse of their brand in domain names, impressing the magnitude of legal recourse and awareness of brand protection in its readers ?.
- **Typosquatting- URL hijacking** : This involves registering domain typographical errors for well-known domains so that the traffic from users making URL entry mistakes goes to them. For example, "goggle.com" replaces "google.com," which leads to a site with an abundance of pop-ups and ads, most likely leading to malware infections from phishing or other malicious activity emanating from exploiting these errors ?. One of the US healthcare providers, Elara Caring, gives an illustrative example of a cyberattack it encountered in December 2020: as a result, the following breaches in healthcare cybersecurity were defined: unauthorised access to email accounts of staff members. The breach, which lasted for a week, underscores the need for an improved incident response ?.
- **Reverse Domain Name Hijacking** : is the act of trademark owners trying to take a domain away from its rightful holder based on the claim of trademark rights, considering that he holds a bona fide registration over the said domain. It may also be described as the use of legal or dispute resolution mechanisms to try to force people from their domains ?. An RDNH was claimed in a UDRP action against "groovle.com," in which the domain was purported to be too close to Google's trademark. However, since the domain was used for another search engine, it was deemed legitimately used and did not violate Google's trademark or be registered in bad faith ?.

6.1.3 Homograph attacks

The risk of continued homograph attacks is in using characters that look similar and thus mimic trusted domain names, such as using a lowercase "l" (el) to look like an uppercase "I" (eye) in the name "paypal.com" vs. "paypal.com". The introduction of International Domain Names has only expanded the scope of such attacks, yet their prevalence is less.

Still, the growing trend of more and more phishing attacks and how easy it is to fool users by taking them to fake sites require eternal vigilance. As a result of a new study, "Cutting through the confusion" [?], it is going to reveal the scale and potential threat to homograph attacks, such as visual similarity between characters from different scripts, like Cyrillic or Greek, which is displayed in punycode in browsers, when attackers register domains that are visually similar to legitimate ones. This can be summarised in the table below, showing possible and actual registrations of such deceptive domains; hence, bringing out the difference between potential and actual use of the deceptive domain. For example, the domain "yahoo.com" had more than 5000 potential homograph variants, with only two actually registered, and "google.com" had a thousand possibilities, with four actual registrations. This is indicative of the importance of developing early preventive development and raising awareness of the risk from homograph attacks, as it sets into a very necessary chain of understanding mechanics and scope of homographs prevalence.

This table will be added in order to clearly show, by means of a graphic illustration, the scope and scale of homograph attacks, which point to the potential risks that these attacks could pose to online security and the awareness and mitigation strategies that need to be put in place for protecting internet users from such deceptive practices. Its noteworthy contribution will be added to the body of knowledge about how homograph attacks are leveraged and their prevalence across various high profile domains.

rank	authoritative domain name	# possible confusables	# registered confusables	confusable names (confusable characters underlined, IDN punycode in parenthesis)
1	yahoo.com	5,202	2	y <u>ah</u> oo.com (xn--yhoo-53d.com), yah <u>o</u> .com
2	msn.com	12	1	m <u>s</u> n.com (xn--mn-eoc.com)
3	google.com	1,156	4	g <u>o</u> ogle.com, go <u>o</u> gle.com, g <u>o</u> g1e.com, go <u>o</u> g1e.com
6	passport.net	19,584	1	passp <u>o</u> rt.net
8	ebay.com	252	2	<u>e</u> bay.com (xn--bay-qdd.com), <u>e</u> bay.com (xn--by-7kcs.com)
11	microsoft.com	48,552	5	micr <u>o</u> soft.com (xn--microsoft-qbh.com), microsoft.com (xn--microsf-sbh.com), micr <u>o</u> soft.com (xn--microsf-djgb.com), micr <u>o</u> soft.com (xn--mrft-65das6nf.com), micros <u>o</u> ft.com
12	amazon.com	3,672	1	amaz <u>o</u> n.com (xn--amazn-mye.com)
18	fastclick.com	1,344	0	
20	aol.com	204	2	a <u>o</u> l.com (xn--al-jbc.com), a <u>o</u> l.com (xn--al-fmc.com)
22	go.com	17	0	
102	bankofamerica.com	25,909,632	1	b <u>a</u> nkofamerica.com (xn--bnkofamerica-x9j.com)
980	paypal.com	3,456	4	pay <u>p</u> al.com (xn--pypal-4ve.com), pay <u>p</u> al.com (xn--papal-fze.com), pay <u>p</u> al.com (xn--paypl-7ve.com), pay <u>p</u> al.com (xn--pyal-53d1h.com)

Figure 6.1: confusables registered for popular domains, adapted from [?].

6.1.4 Real-life Mitigations

The following scenarios are examples of real-life confusable domain mitigations :

- **Cloudflare's Zero Trust Services Approach** : The Cloudflare Zero Trust Services

stops the domain used to mimic the real domain by equipping businesses with anti-phishing protection through Cloudflare Gateway. This protects corporate networks from phishing, using the trust element of well-known brands ?. This is initiated in the system when making the very first query to any domain through a DNS resolver of 1.1.1.1, which in turn initiates a fuzzy matching protocol for analysis and comparison with a database of potential phishing domains. This should issue alerts on domains that are similar to those of legitimate brands, hence easily detecting them promptly and for quick response. Cloudflare enables monitoring 24/7 in real time with historical analysis, offering security teams the alert of domain matching certain patterns, hence being suspected, for fast review and action if the domain has shown up within 30 days. Cloudflare further supports with criteria to specify the corresponding investigation in .json, based on given domains or patterns, and may be subject to security risks.

- **IDN Handling of Google Chrome** : Google Chrome enforces an IDN (Internationalised Domain Names) policy to determine in which Unicode or punycode form a domain label should be displayed. The domain label is tested to determine whether it has mixed script, invisible characters, or visually confusable characters, and whether it is actually validly converted to Unicode. For instance, domains containing characters of different scripts, or those that are clearly identified as mixed script confusables, will be displayed in punycode, warning the users of potential deceptions. Chrome also offers comprehensive warnings for secure URLs that appear to be an imitation of already known Web pages ?.

6.1.5 Techniques for Mitigating Confusable Domains

Mitigating confusable domains requires sophisticated techniques tailored to address the unique challenges presented by both non-Internationalised Domain Names (non-IDNs) and Internationalised Domain Names (IDNs). This differentiation is significant due to the distinct nature of the threats they pose and the technical feasibility of the mitigation strategies applicable to each. The following is a detailed examination of mitigation techniques, along with discussions of the operational feasibility and potential collaboration frameworks involved.

Non-IDNs Mitigation Techniques : Strategies focus on identifying and mitigating domain squatting and typo-squatting, where attackers register domains that are typographical errors or close variants of legitimate domains to deceive users.

1. **Registry-Level Measures**: Domain registries can implement checks to prevent the registration of domains similar to existing trademarks or brand names, using algorithms to detect variations and misspellings closely similar to protected names ?.
2. **Trademark Protection Programmes**: Services such as the Trademark Clearinghouse

(TMCH) offer mechanisms for trademark owners to protect their rights by receiving notifications when someone attempts to register a domain that matches their trademark ?.

3. Automated Monitoring and Reporting: Automated systems can continuously monitor domain registrations for names that closely resemble known trademarks or brand names, allowing rapid detection and legal action against infringers ?.

IDNs Mitigation Techniques: The challenge with IDNs lies in the potential for homograph attacks, where attackers use characters from different scripts that appear visually like characters in the Latin script to create deceptive domains.

1. Punycode Awareness and Monitoring: Web browsers and security tools convert IDNs to punycode, a representation that encodes Unicode characters in ASCII. Awareness of punycode and monitoring for suspicious registrations can help identify potential homograph domains ?.
2. Browser-Level Defences: Modern web browsers have implemented defences against IDN homograph attacks by displaying the punycode version of the domain or alerting users when a domain name contains characters from multiple scripts ?.
3. Collaborative Blacklisting and Sharing of Threat Intelligence: Organisations can collaborate to share information on known malicious IDNs, contributing to comprehensive blacklists that can be used by registrars, DNS providers, and end users to block access to malicious sites ?.

6.1.6 Transparency in Mitigation Efforts

The element of transparency in dealing with confusable domains will be a great support in protecting the Internet from mischievous activities such as phishing and trademark infringements. This encompasses a set of practices by domain registries and registrars to identify and publicise those domains that could mislead due to their similarity to legitimate ones. It contains means of transparency, such as publishing lists of those domains to alert the community about possible threats and taking secure measures, if possible.

- **Cloudflare's Zero Trust Services Approach:** Cloudflare's process for identifying and blocking confusable domains should be transparent to its users. This includes detailing the criteria for flagging domains as phishing sites and the mechanisms in place for users to appeal or request a review of blocked domains. By openly sharing the methodology behind their zero-trust rules and how they are applied through the Cloudflare Gateway, trust in Cloudflare's protective measures is bolstered among corporate networks.

- **IDN Handling of Google Chrome:** Transparency from the side of Google Chrome for the display of domain names helps the user understand the risks to his security. How policy could be properly executed, reported, or suggested for changes by the community of users to increase internet safety will also be explained.
- **Typo-squatting Detection Tools:** The similar methodology should be evident in how similar domain names are detected by tools such as DNS twist or URLCrazy and how it could be detected and shared in a proactive security setup, which could also help others in any organisation.
- **Collaborative Efforts and Intelligence Sharing:** The partnership between cybersecurity entities and domain registrars, as well as initiatives such as the Anti-Phishing Working Group (APWG), should prioritise transparency in their operations. This includes the sharing of methodologies for threat detection, the criteria for taking action against malicious domains, and the processes for stakeholders to contribute or access shared intelligence. Transparency in these collaborative efforts ensures that actions taken against confusable domains are fair, understood by all parties involved, and supported by a broad community of internet security stakeholders.
- **Transparency for non-IDN registries :**
 1. Registry-Level Measures: Transparency in level-registry measures becomes a necessity if trust has to be kept between registrants and domain trademark owners. They are published criteria and algorithms used to find variations and misspellings of names submitted for protection. Making these publicly available can then ensure fairness, and feedback in detecting mechanisms is therefore paved for improving them.
 2. Trademark Protection Programmes: Communication is openly clear about all operations; this includes verification and notification. The guidelines make it easier to understand the rights and measures to protect your brand.
 3. Automated Monitoring and Reporting: set by the criteria and thresholds for informing the brand owners about the protection level for their trademark, and thereby will enable improved monitoring.
- **Transparency for IDN registries :**
 1. Monitoring and Identifying Measures for Suspicious Punycode Registrations: All domain registrars and trademark owners, together with security professionals, must adhere to measures on suspicious punycode registrations. Publicising the details of activities carried out to monitor them propagates homographic threats through collective ideas, also in their identification and mitigation.

2. Browser-Level Defences: Web browsers have an important role in the defence of homograph attacks. They have to explain clearly to the user their defence mechanisms, such as ways of displaying punycode domains and ways of raising warnings so that they can be understood and trusted.
3. Collaborative Blacklisting and Shared Threat Intelligence: Threat intelligence should be collaborative, based on a set of criteria, to blacklist domains. Clear rules on how to submit, validate, and remove data can also enhance the fairness and trust in collaborative security efforts.

In summary, transparency in all these mitigation techniques not only builds trust between users, developers, and organisations, but also enhances the collective ability to respond to and prevent threats posed by confusable domains.

6.1.7 Analysis : Feasibility & Practical Challenges

1. Automated Monitoring and Reporting: Feasible; Technology exists to automate monitoring, even though the refinement of algorithms to decrease false positives and negatives from human review can probably not be undertaken with existing resources.
2. Punycode Registration Monitoring: Feasible; This option is feasible and will mainly require the use of existing technology and cooperation that could be initiated with little difficulty between relevant stakeholders.
3. Blacklisting and Threat Intelligence Sharing: Moderately Feasible; Since agreement could be reached on shared platforms and protocols, but they imply strong cooperation and trust among such diverse entities, which is unlikely to be developed fast.
4. Registry-Level Measures: Not Feasible; this would require very heavy coordination and agreement on standards across diverse jurisdictions and registries, very complex in nature and long drawn.
5. Trademark Protection Programmes: Moderately Feasible; They are well-functioning processes under such adequate structures like TMCH and can be learnt while proceeding with experience, but likely to face legal and operational issues.
6. Browser-Level Defences: Not Feasible; While this is technically feasible, it seems rather infeasible soon that user practices will become uniform across all web browsers and that all users will be well trained in various security practices.
7. Cloudflare's Zero Trust Services Approach: Feasible; since well-architected infrastructure and broad adoption have made Cloudflare zero-trust rules simple and effective to deploy, with a balance of security and operational efficiency without seismic root and branch changes.

8. IDN Handling of Google Chrome and Browser-Level Defences: Feasible; Given that Chrome today has an enormous user base and that the groundwork for stopping homograph attacks already exists, it stands to reason that a solution is reasonably possible, meaning not too difficult, within a set timeline, and within the lifespan of any other typical software product.

6.2 Phishing

6.2.1 Real-life examples

Phishing, a cybercrime in which targets are contacted by email, telephone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data, has become increasingly sophisticated. Two notable examples include:

1. InterMed and Spectrum Healthcare Partners fell for a major phishing attack on 44,000 patient data. The InterMed breach involved clinical information for 33,000 patients, specifically names, birthdates, insurance and some social security numbers, from 4 to 10 September. In another case, Central Maine Orthopaedics is reported to have breached 11,308 of their patient record files by unauthorised access to emails that contain personal and clinical details. It is such an incident that really makes it very paramount to strengthen email security and at the same time to provide professional training on data protection ? .
2. Google and Facebook were almost fooled by a group of phishers into a \$100 million sophisticated scam in which they were imitating legitimate invoices from the suppliers. The case is one among many that have caused the vulnerability of technology firms to social engineering and the need for reinforced security, employee training, and verification processes to combat ever evolving cyber threats ?.

6.2.2 Real-life Mitigations

- **Employee Awareness & Training** : Chelsea Technologies has pointed out the importance of training employees to look for spoofing and attachments that are part of phishing methods. Training employees in the way phishers operate is of paramount importance to keeping sensitive information safe ?.
- **Comprehensive Security Measures** : LaptopMD points out that the risk of ignorant searches requires the formulation of policies that make it difficult to land on some sites. In addition to this, the awareness of phisher techniques and browsing issues by employees will greatly save them from being caught in cases of phishing ?.
- **Technological & Human Factors** : Combining technology with awareness,

SecureHIM advises that both should be combined by any organisation to include spam filters and two-factor authentications with the vigilance of employees to detect and eliminate the risks of phishing ?.

- **Awareness against unsolicited emails** : The Centre for Democracy and Technology outlines the training that should be provided to avoid activities such as phishing, including the need not to respond to unsolicited emails even when suspecting anything fishy ?.

6.2.3 Techniques for Mitigating Phishing

Current phishing attack mitigation techniques focus mainly on preventing phishing emails from reaching users' inboxes and discouraging users from accessing phishing websites ?.

1. **Email filters**: It uses algorithms that filter phishing emails, based on the reputation of the sender, the embedding of the link, and suspicious keywords, so that these emails cannot reach the inbox.
2. **Domain blocking**: Take steps to block access from within an organisation's network to known phishing sites so that the organisation's users do not stumble on them accidentally.
3. **User Training**: Train users on how to recognise signs from phishing emails and the risk associated with clicking on unknown links or sharing personal and sensitive information.

The introduction of the Situational Crime Prevention Approach (SCP) ?, which is an idea to understand the detailed thinking process of the offender and the attributes in the environment that allow the attack. This approach seeks to deter potential attackers simply by raising the level of effort and risk involved in an attacker conducting a successful phishing attack with a concomitant reduction in the likely rewards. This method underscores the importance of understanding the criminal's perspective and creating a hostile environment for phishing activities through strategic preventive measures. This method involves these steps :

1. **Increasing the Effort for Attackers**: Implement strong authentication methods and encryption to make it more challenging for phishers to access or spoof legitimate websites or email accounts.
2. **Clarifying User Responsibilities**: Educating users about their role in maintaining cybersecurity, including recognising phishing attempts, and reporting them.
3. **Enhancing Detection Probability**: Using advanced detection technologies and threat

intelligence to identify and neutralise phishing threats promptly.

4. Limiting Phishers' Access: Restrict the amount of publicly available information that could be used to create convincing phishing emails or impersonating individuals or organisations.
5. Discouraging Future Attacks: Implementing punitive measures against identified attackers and sharing information on phishing campaigns with broader communities to prevent repeat offenders.

This measure is designed not only to stop a phishing attack, but rather to create an environment that would lead to the cost-benefit ratio for phishing not so appealing to the attackers. In fact, comprehensive perspectives on addressing phish through the three methods above singularly go to dramatically lower the vulnerability of organisations and individual persons to such acts.

In addition, Phishlimiter ? , which is a new phishing detection and mitigation approach using Software-Defined Networking where it first proposes a new technique for deep packet inspection (DPI) and then leverages it with software-defined networking (SDN) to identify phishing activities through email and web-based communication. This is how it works:

1. Deep Packet Inspection (DPI): Analyses the part of the network packet data beyond basic header information. It inspects the content of the packets for signatures and patterns associated with phishing.
2. Store and Forward (SF) and Forward and Inspect (FI) modes: SF mode temporarily stores packets for thorough inspection before forwarding, while FI mode prioritises immediate forwarding with parallel inspection to reduce latency.
3. Artificial Neural Network (ANN): A machine learning model that classifies network traffic to identify potential phishing activities by learning from known phishing signatures and behaviours.
4. Dynamic adjustment of network flows: Upon detection of a threat, the system dynamically reroutes or restricts traffic to mitigate potential phishing attacks, adapting to new threats in real time.
5. Minimal disruption to network services: Designed to ensure that the phishing mitigation process does not significantly impact network performance, ensuring smooth operation of network services even under threat detection and mitigation activities.

6.2.4 Transparency in Mitigation Efforts

Transparency in cybersecurity, including phishing mitigation techniques, refers to how openly and clearly methods, policies, and procedures are communicated, understood, and accessible

to all involved stakeholders, particularly employees. Here is how transparency can be applied to each of the mitigation techniques described:

- **Employee Awareness and Training :**

Communication: This will consist of clear informing the employees about the kind of threat and how it could mean for the organisation and their role in these defences.

Accessibility: Make people aware that the repository exists, or make the resources easily available for reference. This would include an intranet site or a repository where people could easily access the trends in phishing on the latest and how to respond.

- **Comprehensive Security Measures:**

Policy Publishing: All available policies, especially those related to web browsing, email attachments, and the use of security tools, will be published openly to let employees know about them.

Changes and Updates: Introduce the workforce to changes relating to security measures and how such changes are beneficial and serve as a cover against new hazards.

- **Technological & Human Factors:**

Tool Transparency: Clearly state the tool and the reason for its being in place for security (e.g., spam filters, two-factor authentication), and its work on subduing phishing.

User Control and Visibility: Attempt to give users some form of control or visibility over the security tools through which their work could be affected. Feedback from a blocked phishing attempt could, for example, help to reinforce the training.

- **Awareness against unsolicited emails:**

Open Communication on Threats: Constant updates on new phishing techniques and any other notable attacks are discussed among the industry to be updated.

Best practices: Develop best practices for easy identification and to be visible on how to catch and react to phishing attacks, with graphic examples or checklists.

- **Email Filters:**

The effectiveness of email filtering technology in mitigating phishing attempts is greatly enhanced by transparency in its operational parameters. This helps to make the user understand, starting from analysing the reputation of the sender to the various steps related to decision making of phishing keywords. Continuous improvement builds trust, and perhaps some community members might even wish to

provide feedback on how to improve the performance of the filters or report inaccuracies to the filter system regarding combat against the threats of phishing.

- **Domain Blocking:**

Such measures may include transparency in the criteria of the blacklisting and regular updates in relation to the access to the known phishing sites inside the organisation's network. This implies also setting a clear means for reporting unlisted phishing sites and correcting false positives by stakeholders. Education for users and IT professionals about these measures fosters a culture of cybersecurity.

- **Situational Crime Prevention Approach (SCP):**

The major advantage of the SCP approach is the clear disclosure of both the applied methodology and the results obtained. This is through the explanation of the analysis of the criminal's thought and environmental factors aiding phishing, whereby the stakeholders are enlightened and, therefore, they make efforts to reduce it. The paper discusses how increasing the effort and risk to the attacker, while lowering the rewards, deters crime. Talking with the community helps them continue to improve and adopt ways to make an organisation's security environment dynamic and evolving.

- **Phishlimiter:**

The phishing detection system, such as the DPI integrated with SDN, has the ability to make its operation transparent, may increase user confidence, and preserve system functionality. It could emphasise the reliability and credibility of such a system if the criteria and algorithms by which the system determines a potential phishing attack are clearly spelt out. User feedback, which is positive pushing forward when the system fails in an inaccuracy or missed phishing attempt, to refine. Share those metrics around effectiveness of the system, the number of detected and prevented attacks, to show value. This article looks at some of the challenges, future development, and open directions for work that establishes an effort from the community in the field of cybersecurity.

6.2.5 Analysis : Feasibility & Practical Challenges

1. Employee Awareness and Training : Feasible; Regular training and simulation exercises can be implemented across organisations of any size with scalable online platforms, requiring minimal resources beyond the initial setup.
2. Comprehensive Security Measures :Feasible; The deployment of web filters and secure browsing policies is technically straightforward with existing technology. The main effort lies in continuous update of policies and employee education.

3. Technological and Human Factors: Feasible; The integration of spam filters, two-factor authentication, and secure browsing add-ons is readily achievable with current technology. The human element, continuous employee vigilance, enhances the effectiveness of these tools without significant additional costs.
4. Awareness against unsolicited emails: Feasible; Establishing and communicating best practices for handling suspicious emails involves minimal costs and leverages existing communication channels within organisations.
5. User Training: Feasible; The training of the user's awareness on phishing is practical and beneficial, as it allows giving room for the user to measure the feedback on the effectiveness of training and to give suggestions for improvements that can enhance programme accessibility and user participation.
6. Situational Crime Prevention Approach (SCP): Feasible; sharing information that identifies how an offender behaves and the environment that helps him/her attack. Although presenting this success story is of great value, great care must be taken in the handling of the detailed analyses of criminal tactics to avoid misuse. Community feedback will allow for further development.
7. Domain Blocking: Moderately Feasible; Updating blacklists and dealing with the false positives, which have to be dealt with. This is a mammoth task, especially for relatively smaller organisations with few resources at their disposal. The process demands balance in responding very accurately within a very short time, which can over-stretch resources.
8. Email Filters: Not Feasible; Describing the general criteria and algorithms for email filtering is possible, but full disclosure risks security by enabling attackers to circumvent these measures. Partial transparency can be achieved without compromising the integrity of the system.
9. Phishlimiter: Not Feasible; The complexity and proprietary nature of technologies like DPI and SDN make full disclosure of Phishlimiter's operations impractical. Detailed investigation of operations could compromise security. Keeping up with evolving phishing tactics requires continuous updates, which may not always be promptly disclosed to avoid aiding adversaries.

6.3 Collaboration Among Registrars, Registries, and DNS Collaborators

This collaboration should be achieved with the DNS registry, the registry, and the collaborators. In that way, they can boost common resources and intelligence that can guide

in making the Internet more secure and resilient. This strictly falls within the remit of registries and registrars acting in collaboration to put in place such stringent registration policy with procedures for verification, checking against mimicking existing trademarks or even popular domain names. In this way, the collaboration can even manifest itself through the sharing of sensitive data with regard to domain abuse threats and trends. Databases and threat intelligence platforms are shared amongst stakeholders, allowing them to anticipate and avert most such perils well before they impact netizens. This collective effort will enable the formulation of standards by which to coordinate responses to confusable domain incident reports. Mitigating confusable domains and phishing requires that registrars, registries, and DNS collaborators work in a common effort. This is due to the increasing level of threats and the shared responsibility of all actors involved in the DNS ecosystem. ? To put this into perspective, here are some examples:

1. Recent changes in the contract from ICANN's contracted parties have imposed on registrars and registries new specifications to define DNS abuse, together with clear requirements for the actions to be taken by such parties immediately actionable evidence of abuse is received. This is a major step toward establishing more clarity on the roles that these different stakeholders can play in addressing the problem of DNS abuse and ensuring that there is a common approach to redress ?.
2. The community itself has approved new obligations from ICANN contract parties to further mitigate DNS abuse, demonstrating the will of the community to come together to address DNS abuse issues ?.
3. Efforts like NetBeacon, with the support of the DNS Abuse Institute, are being rolled out to reduce friction in reporting and mitigating DNS abuse. This service solves the current complexities and quality standards associated with the reporting of DNS abuse, as it makes the work easier for the registrars, ultimately narrowing down their scope to the relevant and evidenced report, as well as it underlines the need for cooperation among registrars, registries, and other DNS stakeholders. This is what is capable of saving the Internet and, at the same time, protecting the credibility and confidence of DNS ?.

Real-life examples of entities seeking to block the resolution of DNS names used by bad actors for phishing and other malicious activities, especially in connection with public recursive DNS servers, frequently revolve around matters of control, filtering, or securing internet traffic with various kinds of motivation corresponding to such sectors. Some attempted these efforts at the government, corporate, and individual levels. As typical examples that pinpoint those instances, consider the following:

1. Governmental Efforts to Block DNS Resolutions : Governments may interfere directly with DNS operation to enforce some censorship or block access to particular types of

content. For instance, China uses the Great Firewall for regulation of access to the World Wide Web within their territory, including doing some DNS mismanagement to block unwanted content ?.

2. Corporate and ISP DNS Filtering : DNS filtering can be deployed by companies and even ISPs in a bid to achieve enhanced online security. For instance, Heimdal Security explicates how DNS filtering works as one of the measures to prevent their access to various harmful or inappropriate websites, since it first checks the requests for domains. If some are actually flagged, access is denied, hence maintaining both security and productivity within one's organisation. This approach is very effective for the prevention of phishing and malware attacks because it stops DNS requests towards malicious sites ?.
3. Ad Block DNS Services : Cloudflare discusses how DNS filtering can be used to prevent access to malicious sites and also filter what is harmful or unfit for viewing. This is done at the DNS level to prevent these sites from loading on devices. Cloudflare uses its DNS to filter part of a more prominent access control policy, which is an effort to secure company data and govern what employees will see on the network they manage ? .

On the negative side, attackers are taking advantage of DNS blocking mechanisms to carry out DNS-based attacks. These include using DGAs (Domain Generation Algorithms) for malware communication, using FastFlux techniques for slip-streaming attacks, basically creating malicious newly registered domains (NRDs) that appear benign and legitimate to an outside observer, etc. All this makes it difficult to block bad content at the DNS level, which calls for quite sophisticated countermeasures.

6.4 Benefits of Transparency

Transparency has numerous advantages when it comes to handling confusable domains and mitigating phishing. First, it encourages domain registry owners and registrars to be more accountable to each other by motivating them to take an active role in the identification and removal of confusable domains and phishing websites. Second, openness discourages bad actors who might otherwise take advantage of the anonymity provided by a lack of public monitoring. Third, by making these lists available to the public, registries and registrars enable companies and trademark owners to promptly take precautionary measures to safeguard their brands, including acquiring domain names or pursuing legal action. Transparency also facilitates community-based mitigation initiatives, in which researchers studying cybersecurity and the broader community work together to detect and eliminate dangers. This coordinated effort not only tackles confusable domains, but also considerably

impedes phishing attempts by revealing, and thus reducing, the strategies employed by bad actors. The effectiveness of these tactics is significantly increased by using the collective expertise and attention to detail of the cybersecurity community, resulting in a more secure online environment for all parties involved.

6.5 Drawbacks and Security Concerns

The publication of confusable domain lists, while aimed at enhancing cybersecurity, carries certain drawbacks and security concerns, including implications for phishing attacks. A primary issue is that making such lists public might serve as a guide for bad actors, revealing potential phishing targets. This exposure could allow bad actors to improve their strategies, thus remaining a step ahead of countermeasures. Additionally, the risk of false positives where legitimate domains are marked as confusable poses significant challenges. For legitimate businesses and individuals, being mistakenly associated with phishing can lead to unnecessary scrutiny, legal complications, and damage to their reputation. Furthermore, the tension between transparency and security raises questions about the effectiveness of these disclosures in preventing attacks. While the goal of transparency is to proactively mitigate abuse, including phishing, the vast number of domain registrations and the evolving tactics of domain abuse may diminish the utility of such lists for end users and businesses, potentially limiting their ability to preemptively address phishing risks.

6.6 Limitations of Research Conducted on DNS Abuse Transparency

This section lists a number of significant limitations that were observed during the research. The limitations imposed have had an effect on the extent, complexity, and applicability of the results, indicating potential avenues for future investigation to improve the understanding and efficacy of DNS abuse mitigation measures.

1. **Variability in reporting standards:** A significant challenge encountered was the lack of uniform standards across DNS infrastructure providers, including registrars and registries, regarding the definition of abuse, the thresholds of action, and the manner in which these actions are reported. Such inconsistency has made efforts to collect and compare the data of different entities hard to piece together into one coherent picture for sensible enforcement of DNS abuse mitigation. This diversity highlights the need for standardised reporting standards by contributing to a fragmented view of abuse management procedures.
2. **Limited Availability of Data:** The general lack of transparency reports that are

available to the public. Many providers either don't release these reports at all or do so in a way that leaves out important information that has to be thoroughly examined. Due to the restricted breadth of research due to this data availability issue, there may be gaps in our understanding of the entire range of DNS abuse management strategies. One major obstacle to evaluating the efficacy and transparency of the abuse mitigation techniques used by various parties is the lack of data.

3. **Reluctance to Share Sensitive Information:** Information provided by respondents about abuses and what they do to mitigate them. In general, concerns about privacy, security, and the potential of revealing vulnerabilities to bad actors contribute to this reluctance, which leads to Limiting the capacity of researchers to perform a comprehensive analysis of DNS abuse mitigation strategies.
4. **Dynamic Nature of DNS Abuse:** The evolving tactics employed by those who abuse DNS are constantly changing, so results can be out of date very fast. It is more difficult to create best practices that are applicable and efficient over time due to this quick change. Because DNS abuse is dynamic, it requires ongoing research and strategy adaptation to stay ahead of new threats.
5. **Potential Bias in Self-Reported Data:** Self-reporting in transparency reports can still bias the results. Organisations have a tendency to emphasise their achievements while downplaying their shortcomings or difficulties. Due to this biased reporting, opinions about how well DNS abuse is being controlled can be distorted, which could cause mitigation efforts to be overestimated.
6. **Complexity of Measuring Impact:** The evaluation of the efficacy of DNS abuse mitigation techniques is hampered by the nature of the Internet ecosystem. The evaluation procedure is further complicated by the indirect relationship that exists between specific actions taken to combat DNS abuse and larger effects, making it challenging to gauge the effectiveness of these efforts.
7. **International and Jurisdictional Challenges:** Due to the international scope of the Internet, different legal and regulatory frameworks in different jurisdictions have an impact on DNS abuse and how it is mitigated. These differences highlight the need for cross-border cooperation and harmonisation by adding complications to the implementation and evaluation of transparent practices on an international scale.
8. **Ethical and Privacy Considerations:** Ethical issues related to data collection and analysis that may include sensitive or personally identifiable information must be addressed in research in this field. Respecting ethical and privacy standards is very important, but it can also restrict the available research approaches, further limiting the breadth and depth of the study.

All of these limitations point to the complex difficulties in conducting thorough research on DNS Abuse Mitigation Transparency. Teamwork, creative thinking, and a commitment to improving research techniques and methods in this developing subject will be needed to address these problems.

6.7 How well did the project meet the objectives?

In evaluating the success and impact of the research project on DNS Abuse Transparency, a key question in assessing the achievements and influence of the study on DNS Abuse Transparency is addressed. To what extent did the project fulfil its original objectives? This section seeks to systematically evaluate the project's accomplishments in relation to its objectives, taking into account the intricate domain of DNS abuse and the difficulties associated with improving transparency and management procedures. A thorough review is provided by looking at stakeholder participation, the contribution to understanding DNS abuse, the objective achievement, and the practical consequences of the results.

Shortcomings are acknowledged and recommendations for further research and development are made, recognising both the successes and the areas that still require improvement. This reflection not only demonstrates the progress gained but also the continuous path toward a DNS ecosystem that is more open, safe, and resistant to abuse.

6.7.1 Objective Fulfilment

The project's goal was to improve stakeholder awareness and transparency about DNS abuse management. Despite encountering obstacles including inconsistent reporting guidelines and restricted data access, the effort succeeded in bringing to light significant flaws in the methods used to mitigate and handle DNS abuse. It revealed the complexity and diversity of processes across various institutions, underscoring the urgent need for standardised reporting requirements.

6.7.2 Impact on Understanding DNS Abuse

Given the difficulties, the research project provided insightful information on the state of DNS abuse mitigation. It demonstrated how DNS abuse is dynamic and how quickly changing bad actor tactics require mitigation measures to be updated on a regular basis. The research highlighted gaps in current understanding and management methods by highlighting the lack of transparency reports and providers' reluctance to provide sensitive information. These discoveries can act as a starting point for future studies and the formulation of policies.

6.7.3 Stakeholder Engagement

It was essential to interact with stakeholders such as registries, policymakers, and DNS registrars. The project encouraged discussion of the need for increased sector and jurisdiction cooperation and transparency. On the other hand, it appears that there is room for improvement in the influence on stakeholder behaviours and policies, particularly in terms of encouraging more proactive engagement and teamwork in the fight against DNS abuse.

6.7.4 Practical Implications

The project's outcomes have beneficial consequences in improving the transparency of DNS abuse mitigation. If put into practice, suggestions for creating uniform reporting guidelines and improving data exchange procedures may result in more efficient and cohesive methods for mitigating DNS abuse. These recommendations provide practical next steps for stakeholders to better address the issues raised.

6.7.5 Suggestions for Improvement

Deeper insights may be obtained for next projects by focusing study questions on newly developed DNS abuse strategies and investigating more aspects of transparency. Improving the methods for engaging stakeholders, perhaps by creating more inclusive forums or working together on joint research projects, could increase the scope and quality of the information collected. Furthermore, promoting the idea of the project could lead to more noticeable changes in practice and policy.

6.7.6 Future Vision

This research project embarked on an extensive effort to clarify the complexity of the transparency of DNS abuse. Taking into account obstacles such as the dynamic nature of abuse methods and the availability of data, the effort achieved significant achievements in highlighting important areas for development and setting the stage for future breakthroughs. The initiative is an essential move toward a more transparent and uniform strategy to mitigating DNS abuse, acknowledging the contributions and the need for continued research and cooperation. To move forward, all parties involved must work together to accept the recommendations and create a more secure, safe online environment.

7 Conclusion

7.1 Brief Review

This project looked at DNS abuse, a situation in which malicious actors exploit domain names for malicious activities such as phishing. DNS infrastructure providers, including registrars and registries, have been the focal points of attention due to their significant roles in controlling and potentially reducing this abuse. The investigation included the complaints these providers receive and the measures they take to mitigate abuse, such as the deletion or blocking of domain name registrations. A critical aspect of this research was the concept of transparency: the extent to which these actions are disclosed and documented by the providers. It was found that the practice of issuing comprehensive transparency reports is not as widespread as necessary, despite the crucial role that openness plays in fostering trust and accountability in the digital realm.

7.2 Main Results

7.2.1 Related back to Project Objectives:

The project led to the identification of serious transparency gaps in the mitigation of DNS abuse adopted by infrastructure providers. Although some reporting and communication measures of mitigation action against DNS abuse have been adopted to trace the information on the mitigation measures undertaken, it is largely inconsistent. This goes hand in hand with our first objective, to better understand practices on transparency in the area and set a clear requirement for standardised transparency measures.

7.2.2 Summary of Proposals:

Throughout the research project, several strategies have been discovered to improve transparency:

1. Regular Transparency Reporting: Urge all DNS infrastructure providers to release reports on a regular basis describing the steps they have taken to mitigate DNS abuse.

2. Stakeholder Engagement: Encourage more cooperation and communication on transparency regulations between DNS providers, users, and legislators.
3. Public Accountability Mechanisms: Provide and implement systems that allow the general public to monitor and evaluate DNS abuse mitigation efforts.
4. Innovation in Defence Strategies and Sharing: Emphasise the importance of preparing new methods to combat DNS abuse by developing and encouraging the sharing of these innovative strategies among stakeholders.
5. Transparency in Monitoring and Collective Action: Encourage open observation of DNS activity and cooperative efforts from all parties within the DNS ecosystem to ensure a unified strategy to mitigate abuse.

These strategies seek to expand on the fundamental measures outlined in this research project, focusing not only on the individual efforts of DNS infrastructure providers but also on the collective efforts and shared responsibilities throughout the DNS ecosystem. By using these tactics, the Internet community can work towards improving trust and transparency, which will result in a DNS system that is more secure and resistant to abuse.

7.2.3 Assessment of Contribution :

These results can be used to show the importance of the application, as the responsibility may fall on the DNS infrastructure providers to have a better and more transparent practice in mitigating DNS abuses. Eventually, the adopted strategies give a chance for better accountability and greater trust from the interested users and parties. In the larger context of cybersecurity and Internet governance, where transparency is becoming more widely acknowledged as essential to promoting a safer online environment, this contribution is vital.

7.3 Future Work

7.3.1 Further Research Directions:

Future research should examine how AI and machine learning are combined to detect predictive DNS abuse and how well international regulatory frameworks enforce transparency requirements. In addition, further research may examine how user trust and behaviour are affected by transparency, as well as how various degrees of openness influence how DNS infrastructure providers are seen. Furthermore, studies could assess how well different transparency techniques mitigate DNS abuse in the real world.

7.3.2 Practical Next Steps for Developing Transparency Best Practices:

1. **Framework Development:** Collaborate with leading industry players to develop a uniform transparency framework that DNS infrastructure providers can use anywhere.
2. **Technology Solutions:** Looking into technical options that automate the gathering and sharing of DNS abuse data to improve transparency.
3. **Policy Recommendations:** Draughting policy suggestions should require transparency in these activities to encourage legislative support for DNS abuse mitigation initiatives.
4. **Stakeholder Collaboration:** Governing bodies that maintain the DNS infrastructure, regulatory organisations, and cybersecurity communities need to join hands to combat and find an amicable solution to these challenges.
5. **Transparency Standardisation:** Standardise transparency reports across the industry to ensure uniformity in disclosing DNS abuse mitigation efforts.
6. **Real-Time Monitoring:** Implement real-time abuse monitoring dashboards to enable swift detection and response to DNS threats.
7. **Public Awareness:** Promote user education on DNS security to enhance public awareness and safeguard against potential abuses.

7.3.3 Enhanced Transparency Practices for DNS Abuse Mitigation:

Building on these initial steps, registries and registrars are urged to implement improved transparency measures such as the following to strengthen the DNS ecosystem's resistance to abuse:

1. **Public Reporting:** Establish detailed and consistent transparency reports that provide information on the number of DNS abuse reports received, the steps taken, and the results of those steps. In addition to increasing user trust, this transparency makes the organisation responsible for efficient abuse mitigation.
2. **Stakeholder Engagement:** Provide forums or advisory committees to discuss and evaluate mitigation solutions for DNS abuse that involve a wide range of stakeholders, such as government representatives, cybersecurity professionals, and members of civil society. This guarantees that decision-making procedures take into account a wide range of points of view.
3. **Abuse Point of Contact:** Clearly identify the abusive contact and make it public. This

makes it easier for the community, including end users and cybersecurity researchers, to report and handle abuse problems effectively.

4. **Best Practice Sharing:** Encourage a transparency environment by sharing best practices, resources, and innovations to mitigate DNS abuse with colleagues in the DNS ecosystem. Workshops for the entire industry or collaborative platforms can help to promote this conversation.
5. **User Education:** Recreate and distribute instructional materials to help domain owners and end users identify and stop DNS misuse. Empowering people with knowledge can drastically reduce the effectiveness of phishing and other abusive techniques.
6. **Automated Abuse Detection:** Make use of AI and machine learning technology to automatically identify possible DNS abuse behaviours. Exchange anonymous indicators of compromise (IoCs) with reliable partners to increase the resilience of the ecosystem as a whole.

7.3.4 Future Directions in DNS Abuse Mitigation:

Future studies and practical initiatives should focus on the following areas to better address the dynamic nature of DNS abuse and proactively counter new threats:

1. **Emerging Technologies:** Exploring the possibility of DNS abuse and creating focused mitigation solutions in AI-generated content and the growth of IoT devices.
2. **AI and Machine Learning for Proactive Defence:** Using data analysis to find possible abuse vectors and advancing AI and machine learning models to anticipate and handle DNS abuse before it happens.
3. **Enhanced IoT Security:** Establishing security guidelines for IoT device makers to stop device exploitation in DNS abuse, encouraging industry-wide adoption through partnerships and laws.
4. **Global Policy and Regulation Dialogue:** Participating in policy discussions to coordinate mitigation measures for DNS abuse and promote laws that promote security, privacy, and openness.
5. **Transparency Evolution:** Advancing transparency standards in line with technology, emphasising real-time data sharing, blockchain-based log reporting, and user-friendly interfaces to prevent unauthorised access to data.

7.3.5 Contributions to Future Transparency Practices:

This research contributes to the ongoing development of best practices for transparency in DNS abuse mitigation. By emphasising the significance of transparent, consistent reporting and promoting stakeholder interaction, it seeks to enable better informed policy-making and promote a safer online environment. Identifying existing challenges and proposing feasible solutions, this study is a first step toward improving openness in the DNS ecosystem. The desired results are a reduction in DNS abuse, an informed and active user base, and the development of a more reliable Internet ecosystem.

7.4 Reflection

7.4.1 Personal Learning:

With this project, I have appreciably learnt the complexities of DNS abuse and how these complexities could pose a challenge in conceiving systems that address the potential lack of transparency. In that sense, DNS abuse is said to be very dynamic, always changing to expose new tactics by bad actors; mitigation strategies should, therefore, become adaptive. I learnt that transparency isn't just about sharing information; it is about building trust within the community, improving the effectiveness of abuse mitigation efforts, and impacting broader internet governance and security positively.

7.4.2 Evaluation of Research Process:

In other words, this research project has brought to light the complicated hurdles in studying DNS abuse mitigation transparency, from the reluctance to share sensitive information due to privacy and security concerns to possible biases in data self-reporting. The process made clear the delicate balance that must be struck between maintaining security and releasing just enough information to be transparent. Although the technique allowed a thorough analysis to be performed, it also highlighted areas that needed to be improved, such as determining more accurate ways to assess how transparency practices affect the reduction of DNS abuse.

7.4.3 Perspective on Research Findings and Contributions:

This research project offers a more comprehensive view of current procedures and their effectiveness, contributing to ongoing conversations on the mitigation and transparency of DNS abuse. Through gap analysis and practical strategy recommendations, the study highlights the necessity of a coordinated approach to openness. It calls for the creation of guidelines and best practices that improve cooperation between all parties involved in the

DNS ecosystem. While great progress has been made, my work emphasises the ongoing need for attention and effort in this area and suggests that the road towards a more transparent, safe, and abuse-resistant DNS landscape is far from over.

In summary, this project has improved my knowledge of DNS abuse mitigation and the pursuit of transparency, while also providing insightful information that will guide future research in this area of cybersecurity and Internet governance.

A1 Appendix

The Domain Name System (DNS) plays a role in the infrastructure of the Internet by converting user domain names into IP addresses. However, due to its use and importance it has become a target for actors seeking to exploit it. These abuses range from setting up phishing websites to taking advantage of DNS for activities such as typosquatting. The responsibility for mitigating abuse primarily lies with DNS infrastructure providers, such as registrars and registries. These entities respond to reports of abuse by taking down confirmed domain names or proactively blocking the registration of harmful ones. While these actions are essential for maintaining the security and integrity of DNS, they also raise questions about how transparent these measures are.

Transparency in the context of mitigating DNS abuse refers to the disclosure of actions taken by registries and registrars including the criteria and reasoning behind their decisions. Currently, there is a prevalence in publishing transparency reports related to this matter, leading to a lack of clarity and understanding about the processes involved in combating DNS abuse. This project aims to address this issue through a survey involving registries, registrars, and other stakeholders actively engaged in mitigating DNS abuse.

The main objective of the survey is to collect, organise and describe the transparency reports they are presently accessible. This will help us gain an understanding of the status of transparency, in mitigating DNS abuse.

A1.1 Appendix numbering

Appendices are numbered sequentially, A1, A2, A3... The sections, figures and tables within appendices are numbered in the same way as in the main text. For example, the first figure in Appendix A1 would be Figure A1.1. Equations continue the numbering of the main text.