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 14, 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 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 always been critical due to the growing reliance on the Internet for both personal and professional activity. To promote a safer online environment, this project investigates whether and if so, additional transparency related to DNS abuse mitigations might help improve the overall DNS ecosystem. Every type of abuse puts users at risk by making identity theft, money loss, data breaches, and system intrusions easier, as well as undermining confidence in online services. The research project emphasises how urgent it is to address these problems because new technologies such as IoT and AI have the potential to worsen them.

The methodology used in this study included a thorough examination of the DNS ecosystem, vulnerability identification, and an assessment of mitigation initiatives that are currently being implemented by important parties, such as registries and registrars. The survey of DNS infrastructure providers and stakeholders was part of the selective survey 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 the openness of DNS abuse mitigation initiatives. Although several organisations have taken positive steps toward transparency, there is still a lack of standardisation and fragmentation in the industry as a whole. The report makes several suggestions to improve openness and transparency, such as creating uniform reporting guidelines, encouraging greater cooperation between DNS stakeholders, and implementing best practices to deal with DNS abuse openly and transparently.

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 transparency, which we hope will result in a more secure and reliable Internet.

Acknowledgements

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

First, I would like to thank God. Everything I do is done with your 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.

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 mitigation 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.

I want to take this time to show my sincere thanks to friends and college friends who have made good company, understanding the times of stress and relief during our college years. Their presence and support have been a great joy and motivation.

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

List of Figures

List of Tables

1 Introduction

1.1 Brief Context for the Problem

The Domain Name System (DNS), as seen in Figure 1.1, translates domain names into IP addresses. This will definitely affect the daily digital interaction of each user, along with the smooth running of the Internet. Unfortunately, this one is not resistant to abuse. Meanwhile, malicious actors use DNS domains for a variety of abusive and sometimes illegal activities, such as sending malware, phishing websites, and controlling botnets [6]. Therefore, such activity undermines the reliability and security of the Internet, posing very serious risks to cybersecurity and user trust [7]. Addressing this issue requires a robust response from DNS infrastructure providers, including registrars and registries, who play a role in the management of abuse complaints. Registries refer to organisations that function to manage the top-level domains (TLDs) of the Internet, such as ".com" and ".net". On their part, registrars play a role as some form of intermediaries in the sale of domain names to the members of the public. Entities of this kind have the power to disable or deny the registration of DNS names that have been found to be abusive. But it will also consider proactive measures, such as turning down registrations that may facilitate "typosquatting", and potentially regulating permissible domain names to censor registration or renewal based on content. This would enhance the efficiency of such interventions since they shall have been transparent on the measures and the justification thereof. Although the trend is in a manner that issuing transparency reports would be able to shed light on the practices, this happens on rare occasions.

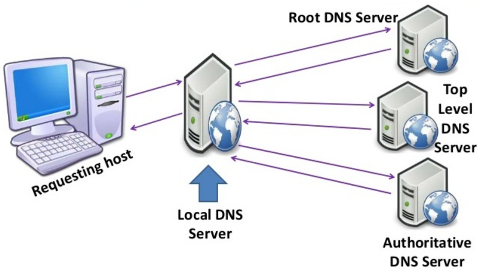


Figure 1.1: How DNS works. Adapted from [1].

1.2 Motivation

With the growing opportunities for DNS abuse for malicious and sometimes even illegal activities such as confusable domains and phishing, the figure 1.2 of honesty and protection is at issue. This has been particularly highlighted by the harshness and regularity with which this occurs in recent studies: such as the "Study on Domain Name System (DNS) Abuse: Technical Report" by Bayer et al., which represents the need for more surveillance and moderation activities [7]. Many instances of DNS abuse have not only jeopardised user protection but also shattered public trust in the digital market. As citizens become more aware of these hazards, their confidence declines, and there is a pressing need to mitigate the challenges to restore trust and a secure online environment. Hesselman et al. [8], proposed the development of a "responsible Internet" by improving community-level transparency, as well as the responsibility to increase confidence and control. Mathew and Cheshire's analysis and self-reporting Trust and Community Practice in the Context of Network Security explore the importance of trusting interactions and communities online and depict how the danger of DNS abuse undermines it [9].

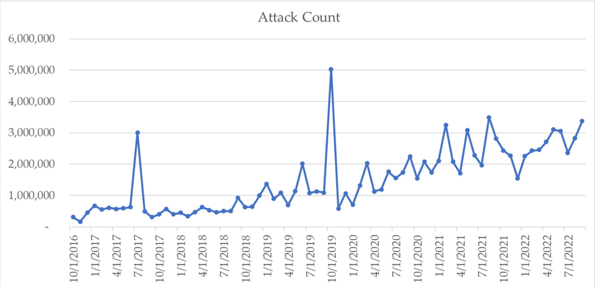


Figure 1.2: increase in DNS abuse incidents over time. Adapted from [2].

Registries and registrars are leading the way in this issue, especially DNS infrastructure providers such as registrars and registries. However, their policies are probably clear and transparent to themselves, just not to outsiders. This clear approach to handling DNS abuse allegations and their accompanying actions worsens the ongoing lack of confidence. Identified in this case are the credibility and a necessary need to protect the Internet [10]. It also covers the moral and legal implications, in addition to technical aspects of DNS abuse and how one can mitigate it. This is the void to which the project is motivated to fill by exploring ways to increase the transparency of mitigation of DNS abuse. To understand current efforts, the research also sought to find the difficulties in the way of more transparent practices through an evaluation of the current landscape on transparency reports and practices among DNS infrastructure providers. The ultimate goal is to contribute to a system that can facilitate, promote, and enable better and more efficient approachable transparency in the mitigation of DNS abuse.

1.3 Research Question/Project & Personal objective

1.3.1 Research Question

Primary research question: "How does the work of registries, registrars, and other DNS infrastructure participants, as it appears in transparency reports, help mitigate DNS abuse, and what can be learnt from it, in terms of best practices for transparency when it comes to handling complaints related to DNS abuse?" 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

- Examine the protocols and measures that DNS infrastructure providers use to respond to abuse complaints.
- Report the most common types of DNS abuse complaint received and the mechanisms applied in most cases.

Assess Transparency Levels:

- Evaluate the level of transparency available in the actions taken by carriers/infrastructure providers against DNS abuse.
- Identify what information is made public, how it is communicated, and the frequency of disclosure.

Evaluating Against Best Practices:

- Measure the results against best practices in the field to establish areas of success and failure.
- Identify examples of good and poor transparency or abuse mitigation measures.

Develop recommendations :

- Suggest actionable recommendations to DNS infrastructure providers to improve their abuse handling and transparency.
- Propose that some policy changes or initiatives be implemented to normalise and enhance such practices across the industry.
- Contribute to work in the future on how best practices for transparency may be developed.

Contribute to stakeholder understanding:

- Give stakeholders, including consumers, policymakers, and other providers, an understanding of the handling and transparency of DNS abuse.
- Develop a roadmap for further research and discussion on improving DNS trust and security.

1.4 Scope

The Scope of this project will consider the transparency measures that registrars and registries take to mitigate DNS abuse. It will look at the collection and characterisation of transparency reports that can be obtained from registries and registrars, among others that are given the same responsibilities to mitigate abuse. Furthermore, this work will review the transparency reports developed in the current year, thus forming future work on the ways through which practices for transparency could be developed. The project discusses with different actors, as summarised in figure 1.3, in the DNS ecosystem to obtain their opinions and insights on what they are currently practising and the challenges they face. This will involve establishing criteria that can be used to measure the way in which the same transparency can affect the perception of the Internet user, which then relates to trust and safety. The new system will not include the creation of new transparency tools or systems, but will be based on the review of current procedures and the recommendation of changes for the better. The key objective of the study is to learn more about transparency and its impacts.

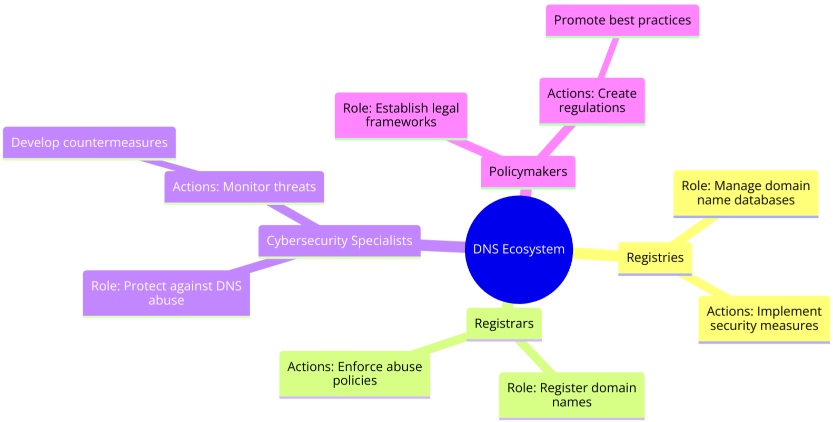

Promote best practices
Actions: Create regulations
Role: Establish legal frameworks
Policymakers
Develop countermeasures
Actions: Monitor threats
Cybersecurity Specialists
Role: Protect against DNS abuse
DNS Ecosystem
Role: Manage domain name databases
Registries
Actions: Implement security measures
Registrars
Actions: Enforce abuse policies
Role: Register domain names

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. The research will first examine the different aspects of DNS abuse, such as popular forms like phishing, confusable domains, etc. and their broader consequences.

The questionnaire will explore the scope and effectiveness of current practices implemented on the aspect of transparency in mitigating abuse associated with the DNS. At the same time, the study will also unveil current transparency reports that reflect the landscape, frequency, scope, and accessibility of the reports to users. Critical evaluation of the handling of DNS abuse reports forms the core of the project.

Critical evaluation of the handling of DNS abuse reports forms the core of the project. This will involve a review of proactive security controls that may be in place, procedures for mitigation, and avoidance of abusive domain registrations. Thereafter, these will be assessed in terms of how transparency influences not only user trust, but also provider reputation, and overall the effectiveness of techniques applied in mitigating abuse. The best practices for mitigating DNS abuse.

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. It is under this background that the research will, therefore, with these findings in mind, develop a set of practical recommendations for the DNS infrastructure providers seeking to increase transparency for better security and, therefore, trust in the digital ecosystem.

A comprehensive timeline will guide the progress, guaranteeing an organised study of the subject. The project, upon completion, would have contributed to a collection of recommendations and considerations for further study and policy creation in this area of Internet governance. This, in turn, would give a further comprehensive understanding of where the current state of DNS abuse transparency lies.

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 discusses the foundation of DNS, its importance, its weaknesses, and several types of abuse. Explaining the methods formulated in combating DNS abuse gives a specific look at the work done by ICANN and the DNS Abuse Institute.

Chapter 3 - State of the art

This chapter critically looks at some of the existing strategies towards mitigation of DNS abuse and their effectiveness. This chapter will give an account of the complex relationship that international governments have with DNS and outline 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. Investigate 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 is the practical part of the project, where all other findings are implemented, including integrating the system, the back-end, and front-end implementations, and implementation technologies that will form the system. The area that this part covers is how the DNS data are visualised with the term of abuse and how the system implementation challenges are addressed. The next section also includes the testing and validation that are performed.

Chapter 6 - Evaluation & Discussion

This chapter evaluates the way the project meets the mitigation of DNS abuse and the improvement of transparency, as well as the chapter was also used to evaluate the effectiveness of transparency in mitigating DNS abuse while evaluating security issues. Furthermore, the chapter will present the limitations of the study and the extent to which the project achieved its objectives.

Chapter 7 - Conclusion

The chapter provided a summary of the project results and recommendations for improving the transparency of DNS abuse mitigation. It is important to note that no matter how difficult the situation, it is important to continue to try to improve the overall security of the DNS. As a result, there are opportunities for further research in the area discussed. More importantly, the chapter underlines the essence of collaboration and transparency in tackling DNS abuse.

2 Background

This chapter will cover the relevant basic information about this project, focusing on the world of DNS abuse and transparency. This will involve a detailed examination of the domain name system and its role in an online community and the many abuses it suffers, a comprehensive history of the policies and established entities used widely to combat DNS abuse, and, in particular, a detailed analysis of the DNS Abuse Institute and what it has achieved. Observing these various methodologies and appreciating their strengths and weaknesses, the reader will get a comprehensive idea of the current DNS abuse situation and the need for a transparent and proactive approach. 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

DNS plays a 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 [11]. The types of security threats vary widely, from DNS infrastructure targeting DDoS attacks to cache poisoning and DNS traffic hijacking. These attacks have the potential to cause damage, including service interruptions, and help with theft and spying. The lack of encryption in standard DNS design makes user query data accessible to abuse and eavesdropping, raising serious privacy concerns. However, weaknesses do not define the end of the story. The same survey also studies new solutions to improve DNS security and privacy. One example of such a new security measure is the deployment of DNSSEC, or DNS Security Extensions, which authenticate the DNS data and ensure their integrity and reliability while resisting some types of attack. Moreover, privacy-enhancing technologies have made it possible for DNS queries to be encrypted to block eavesdropping and information manipulation. They include DNS over HTTPS and TLS. The DNS threats and protection settings change over time in sync with the Internet. Such flaws and current efforts to mitigate them are part of making DNS robust and more reliable. The standard DNS request includes three types of query to speed up the process and reduce the path data length: the first is recursive, where the DNS client takes a direct answer, or an error record not found from the DNS server; the second is iterative, and if the server does not have the answer, it indicates to the client the next server, which can have it, and this happens again and again until the client receives an answer or a dead end; the third is non-recursive, when the DNS server knows the answer because it is directly responsible for this information, or, for example, has it due to the request received earlier. This factor reduces the unnecessary load on the servers involved and ultimately the traffic on the Internet.

2.2 Strategies & Collaborations in Addressing DNS Abuse

The DNS Abuse Institute, which will focus on DNS abuse to help increase security through the domain name system, will focus 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 of making the online environment more secure. Efforts by the institute, such as Compass Dashboards, provide data to registries and registrars that will enable proper decisions in 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 [12]. Another such global strategy against DNS abuse has been contributed by the Internet Corporation for Assigned Names and Numbers (ICANN) [13] 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 [14].

2.3 Different Forms of DNS Abuse

DNS abuse takes many forms, each with its 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 [15].

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 [16].
- **Mechanism:** The deception can be carried out by sending mail or messages about the need to follow the link to a site similar to the real one [17].
- **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 [18].
- **Mechanism:** A user can simply type a typo in the address bar, and the consequences of a visit to this site can be malicious software or an attempt to phish.
- **Impact:** Deception of users and potential harm to brand reputation [19].

2.3.3 Domain Hijacking

- **Description:** Unauthorised acquisition of domain names by exploiting security vulnerabilities in the domain registration system [18].
- **Mechanism:** There are times when the attacker, using social engineering, phishing, or vulnerabilities in the protection of the authorised domain, gains control over it.
- **Impact:** Loss of control of the website, redirection to malicious sites, and potential data breaches.

2.3.4 Botnets

- **Description:** It involves controlling a group of computers infected with malware, used to carry out attacks or spread spam and malware [20].
- **Mechanism:** Once a potential victim's computer is infected, a particularly large number of compromised computers will form a network under the attacker's control.
- **Impact:** Results 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 [21].
- **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:** It generates domain names that act as meeting points for botnets [22].
- **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.

2.3.7 Dangling DNS Records

- **Description:** DNS entry pointing to a resource (like around an IP address or domain name) that is under the control of the owner of the originating domain. This occurs in a scenario where cloud resources are being decommissioned and the respective DNS records for such resources are not updated [23].
- **Mechanism:** These unclaimed DNS entries will then become available for any attacker to set up malicious services on those resources, effectively "hacking" the traffic intended for the services from the original domain.
- **Impact:** Results in some security issues, such as phishing, malware distribution, and data intercepting, which puts end-user information at risk from other cybercrime activities against them and their organisation.

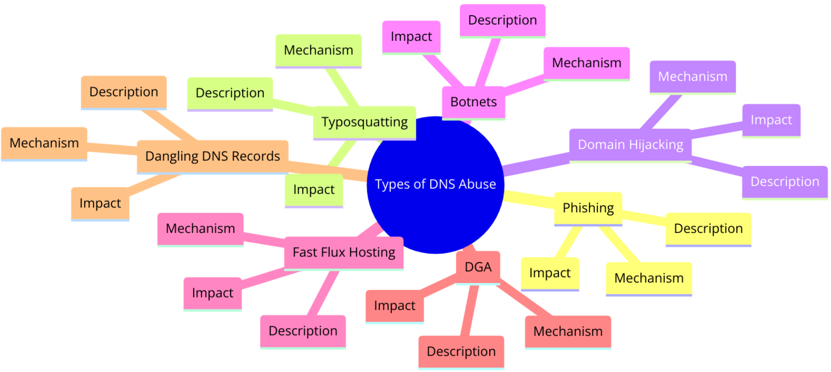


Figure 2.1: Different Forms of DNS Abuse.

2.4 How DNS Abuse Harms Users

The consequences of DNS abuse are severe and cause harm not only to the end-user but also to the organisation, and they are more than basic technological interruptions. Identity theft is one of the most prominent and direct outcomes. For instance, when it comes to phishing, a widely used kind of DNS abuse, people are lured to realistic, but misleading websites; we see how people are led to fake but realistic platforms to get information. Even if it leads to financial theft or unauthorised access to accounts, information obtained through phishing schemes can cause long-term damage to a person's reputation and credit [24].

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 [25].

2.4.3 Data Breach

- **Malware:** Malicious software spread through compromised DNS systems can allow unauthorised access to corporate data, leading to data breaches [26].

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 [27].

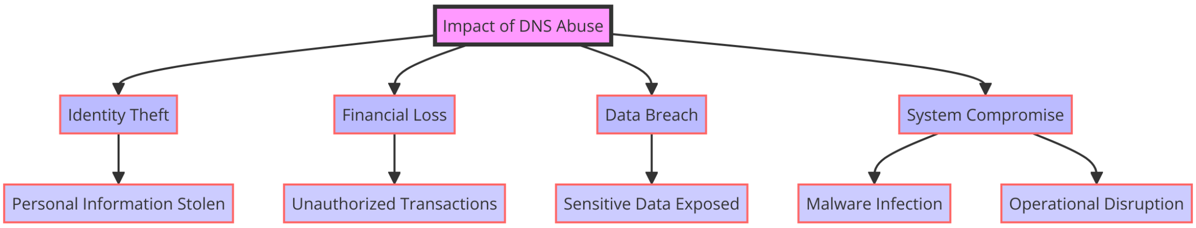


Figure 2.2: How DNS Abuse Harms Users.

2.5 Future Dangers of DNS Abuse

Bad actor strategies and tools evolve along with technological refinements, and the progression of DNS abuse trends could entail new threats in the future. A very important aspect is that the complexity of the attack has increased. Increasing their attacks with more sophistication each time, bad actors find increasingly complex ways to exploit DNS, for example, by developing new, more deceptive phishing efforts or using highly complicated virus dissemination networks [28].

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 [29].

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 [30].

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 [31].

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 [32].

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 [33].

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 [34].

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 [35].

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 [36].

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 [37].

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 [38].

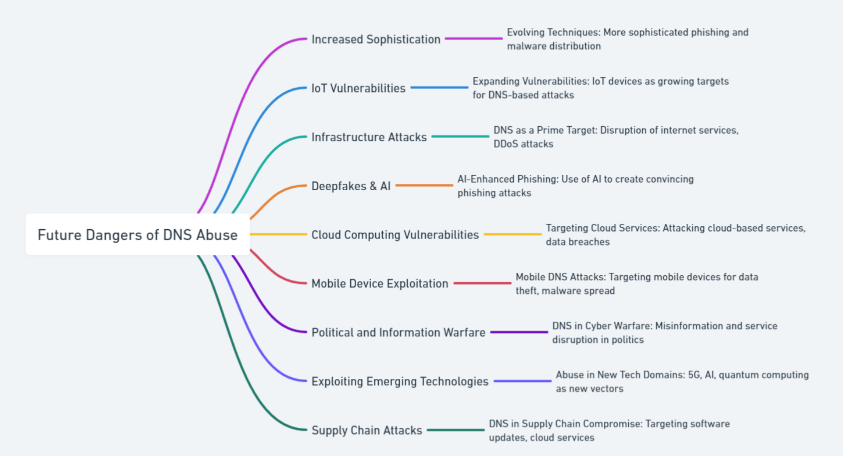

Future Dangers of DNS Abuse
Increased Sophistication
Evolving Techniques: More sophisticated phishing and malware distribution
IoT Vulnerabilities
Expanding Vulnerabilities: IoT devices as growing targets for DNS-based attacks
Infrastructure Attacks
DNS as a Prime Target: Disruption of internet services, DDoS attacks
Deepfakes & AI
AI-Enhanced Phishing: Use of AI to create convincing phishing attacks
Cloud Computing Vulnerabilities
Targeting Cloud Services: Attacking cloud-based services, data breaches
Mobile Device Exploitation
Mobile DNS Attacks: Targeting mobile devices for data theft, malware spread
Political and Information Warfare
DNS in Cyber Warfare: Misinformation and service disruption in politics
Exploiting Emerging Technologies
Abuse in New Tech Domains: 5G, AI, quantum computing as new vectors
Supply Chain Attacks
DNS in Supply Chain Compromise: Targeting software updates, cloud services

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 [39]. To confirm security and ensure that systems have not been compromised, regular audits of DNS configurations and domain registrations are also necessary [40] .

1. **Monitoring & Reporting**
   - Implementation: Use automated systems to monitor domain name registration for patterns that may indicate DNS abuse [39]. Establish procedures for reporting activities to authorities or cybersecurity organisations [40].
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 [39]. This adds a layer of security beyond passwords, helping to prevent unauthorised domain transfers or alterations [41].
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 [42].

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 [43].

8. **Machine Learning**
   - Implementation: Using AI and machine learning algorithms to analyse patterns in DNS traffic and proactively predict instances of DNS abuse [39]. This proactive approach enables the identification of threats before they materialise [44].

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 [45].

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.

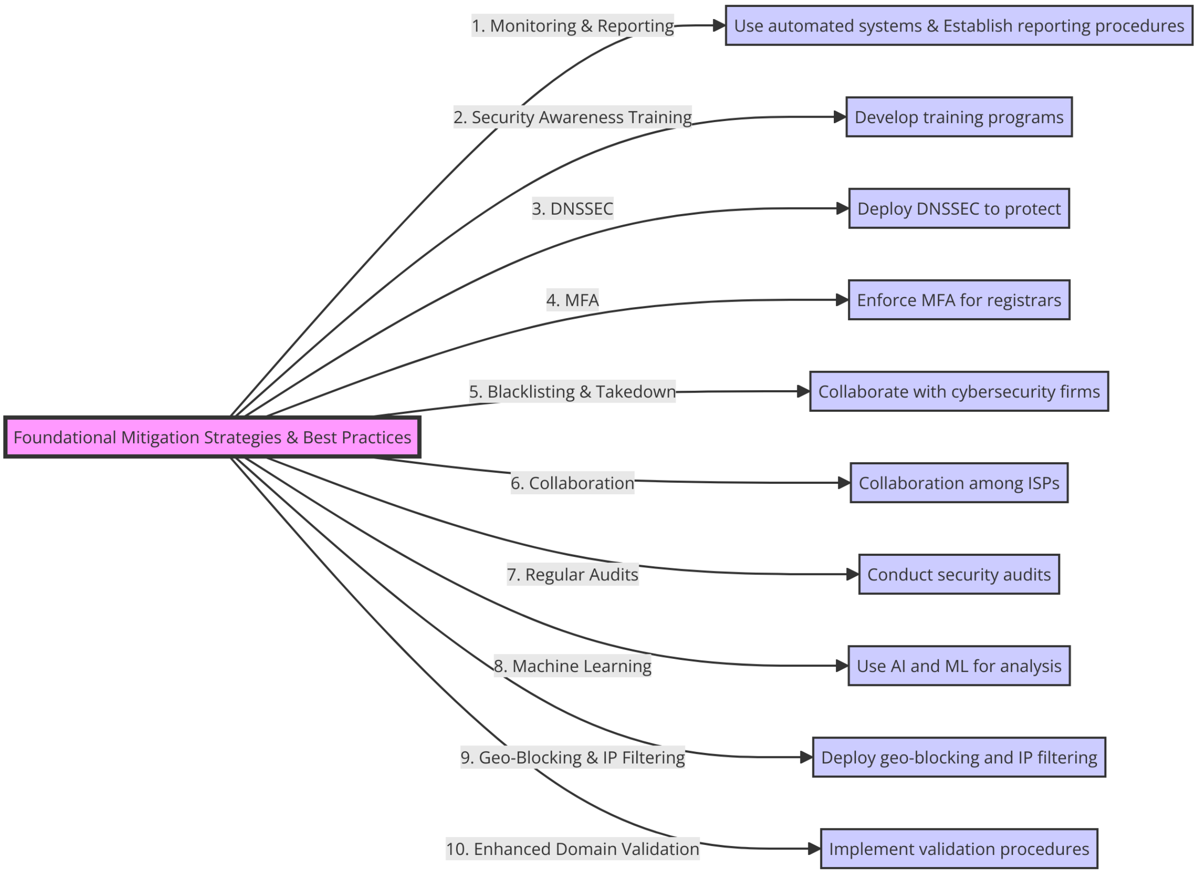

Foundational Mitigation Strategies & Best Practices
1. Monitoring & Reporting
Use automated systems & Establish reporting procedures
2. Security Awareness Training
Develop training programs
3. DNSSEC
Deploy DNSSEC to protect
4. MFA
Enforce MFA for registrars
5. Blacklisting & Takedown
Collaborate with cybersecurity firms
6. Collaboration
Collaboration among ISPs
7. Regular Audits
Conduct security audits
8. Machine Learning
Use AI and ML for analysis
9. Geo-Blocking & IP Filtering
Deploy geo-blocking and IP filtering
10. Enhanced Domain Validation
Implement validation procedures

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, we look at How DNS abuse harms the 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 the 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.
Dangling DNS Records	Service Disruption	Monitoring and Auditing of DNS Records	Regular monitoring allows for the early detection of dangling DNS records, reducing the window of opportunity for attackers.	Promotes proactive security practices and reduces the incidence of service interruptions
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.

Continued on next page

DNS Abuse	User Harm	Mitigation Strategy	Reasoning	Transparency Aspect
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.
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, and potential future threats. Understanding these ranges and the effects they can have is important for the development of regulation and measures. Both the DNS Abuse Institute and ICANN have taken great steps in dealing with this issue. With the advancement of technology and the growing threats, it is more of an adaptive and collaborative approach that remains the key. Possible mitigation techniques that have been discussed outline a guide to the possible approach to combating DNS abuse such as advanced technology, enhanced validation, and continuous monitoring. Cooperation with the use of new technologies is indicated, hence, in DNS abuse mitigation, to reach a joint effort in the management of abuse. Thus, a comprehensive strategy would, of course, call for some appropriate tools, but it would also be a combination of approaches and, most importantly, cooperation from the industry. The evolution of the digital landscape requires adaptable approaches to maintain the security of the DNS and Internet infrastructure.

3 State of the Art

This chapter outlines the methods for mitigating abuse of DNS, and developments in the field, and compares the efficiency and transparency of the various ways to counteract the threat, including DNS filtering, or threat intelligence in which experts bring together and examine relevant information about cyber attacks. Furthermore, the section mentions the recent methods of DNS abuse, such as actions related to domain-generating techniques, as well as DoT and DoH. AI and machine learning are emphasised to detect and counter DNS abuse: The last peculiarities characterise the latter half of the section. It discusses the various directions that require more expertise and solutions and technologies that can advance the prevention of DNS abuse. Case studies present real examples of DNS abuse actions and events.

3.1 Current Strategies and Their Effectiveness to DNS Abuse

DNS abuse presents a challenge to 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. In addition, threat intelligence methodologies use data analysis to identify potential risks, as exemplified by [46]. 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 claims to be committed to maintaining transparency [47], 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 shaping a trustworthy environment in light of addressing Internet safety and privacy concerns. Their approach to handling DNS abuse reports and law enforcement requests are anchored on three core principles:

(a) Due Process: Cloudflare will comply with due process as required by law, remaining neutral and not exceeding legal requirements.

(b) 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 applies to each request.

(c) Notice: Cloudflare will notify customers if legal requests are made for their information unless prohibited by law.

Handling of DNS Abuse and Law Enforcement Requests:

(a) Cloudflare's response to DNS abuse by phishing and malware is decisive action: service termination for non-compliant domains. In the second semester of 2022, a significant number of accounts and domains were suspended because they hosted harmful content.

(b) The legality of such requests is reviewed with strictness by the company, ensuring that required information is provided to the respective bodies within international privacy laws; if they infringe upon user rights, they are rejected.

Challenges and Efforts to Mitigate DNS Abuse:

(a) Cloudflare aims to mitigate DNS abuse, balance free speech with the law, and bring cooperation with all parties through its proactive work.

(b) The company understands the challenge of dealing with DNS abuse, and great effort is made to provide transparency concerning the privacy standards set by the law.

Future Directions:

(a) Cloudflare intends to improve partnership participation and abuse detection systems with due transparency in reporting. They have also redoubled their efforts in the field of education to increase cybersecurity awareness among users and lead reform policies and legal concerns in line with the balance between privacy and law enforcement.

In conclusion, the company emphasises its commitment to protecting legal processes and user privacy while navigating government and law enforcement requests. A significant 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 DNS is in all matters that pertain to the accessibility of content on the Internet and governance of the Internet. Detailed statistics, trends, and specific case studies that formed the basis for their latest transparency reports can be found in the appendix A1.1.

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, concerning 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 pressure 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 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 [48].

3. Amazon Transparency Reports

   This role of DNS in the service of 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 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. 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 [49].

4. 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. DNS serves both as a foundation for the distribution of information online 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 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, in the control of counterfeit, fake, and grey markets, and in protecting the rights of the owner of intellectual property and trademarks [50].

5. 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 on the number and types of request received in 2022, the report puts a heavy emphasis on TMUS's efforts to respect customer privacy and comply 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 [51].

6. 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 [52].

7. Xiaomi Transparency Report: Government Requests for User Information

   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 [53].

8. 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 [54].

9. 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 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 proves that Apple has been pretty guarded in its responses to requests for user data [55].

3.1.2 Effectiveness of Current DNS Abuse Mitigation Strategies

There are various ways in which this abuse can be mitigated. Approaches include the deployment of blocking tools, the knowledge of potential attacks, and the detection of suspicious attempts. DNS filtering is a practice in which access to any particular website is controlled based on predefined rules concerning the result you would obtain based on the background context, and it can occur in multiple forums, e.g., register and registry are such forums where a DNS filtering mechanism would compare DNS names to the block lists and the set of rules then takes the necessary action such as. It could be used to prevent homograph attacks volumetric DDoS attacks DNS filtering mechanisms could be used to compare domain names against block lists and the predefined rule to identify possibly dangerous homographs discussed above. Additionally, threat intelligence contributes to the identification of warning signs and detection of abnormal activities in DNS [56]. This can help to identify and assess potential threats and evil activities early. For example, it can detect similarities that might point to a phishing campaign, domain hijacking, malware distribution, or another form of DNS abuse. To determine the relative effectiveness of each of these methods, their applications must be compared with real-world performance. DNS filtering, for example, might be effective in blocking malicious content. However, it may also allow harmful content to penetrate the filtering process and therefore impact the end-user experience. Threat intelligence is as effective as 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 [57]. 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. In such a setting, the rapid growth and implementation of DNS over TLS (DoT) and DNS over HTTPS (DoH) constitute a double-edged sword. While the above encryption protocols were intended to increase privacy and security by encrypting DNS questions, they also incidentally provide threat actors with a means to mask malicious traffic, thereby increasing the threat surface. The above can be pointed out in various facets, from personal devices to organisational networks. For example, malefactors might employ DoH and DoT in the enterprise context to bypass obsolete security safeguards and create concealed communication links. In addition, domain generation algorithms (DGA) are of great importance in cyber threats, generating a massive number of random domain names automatically, making it difficult to locate and deactivate threat-promoting websites [58]. This method, which is an integral aspect of botnet command and control (C2) operations, complicates the efforts of cyber defence systems to anticipate and identify dangers.

The benefit of enabling DoT and DoH is to improve the level of current privacy by avoiding DNS query surveillance and encrypting DNS traffic, which reduces the likelihood of intercepting or manipulating data by bad actors. However, such protocols do give attackers a means to hide their malicious activities, which in turn poses problems to traditional DNS security systems when trying to detect and deflect harmful content. This could cause such protocols to unintentionally bypass content filtering policies and, therefore, give way to potential security breaches within the organisational environment. On the other hand, DGAs enable bad actors to avoid detection and keep their C2 communication channel open because dynamically produced domains are impossible to forecast and block on a preemptive basis. As a result, numerous domain names will become available to security facilities to monitor, making the intelligence task more difficult and requiring consistent focus and blacklist updates. Given that both methods have achieved substantial use, cybersecurity practitioners are encouraged to take a proactive and educated position, recognise the potential for exploitation of these patterns, and establish comprehensive procedures. Those should take into account the advantages of encryption and domain generation, as well as the requirement to combat DNS-based abuse on all digital fronts.

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 [59]. 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 blackhole 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. This type of transparency is key, as it helps build trust, is open to accountability and fosters an environment conducive to the collaboration of stakeholders that will allow a more effective fight against abuse in the DNS ecosystem, as illustrated in the figure 3.1 below. This transparency enables us to understand the predictions of the models, the opportunity to map the data used when training the model, and how to understand the methods that underlie the decision, as highlighted in [60]. The problem lies in the fact that the complexity of modern predictive models and their simplicity of interpretation are very sensitive. 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.

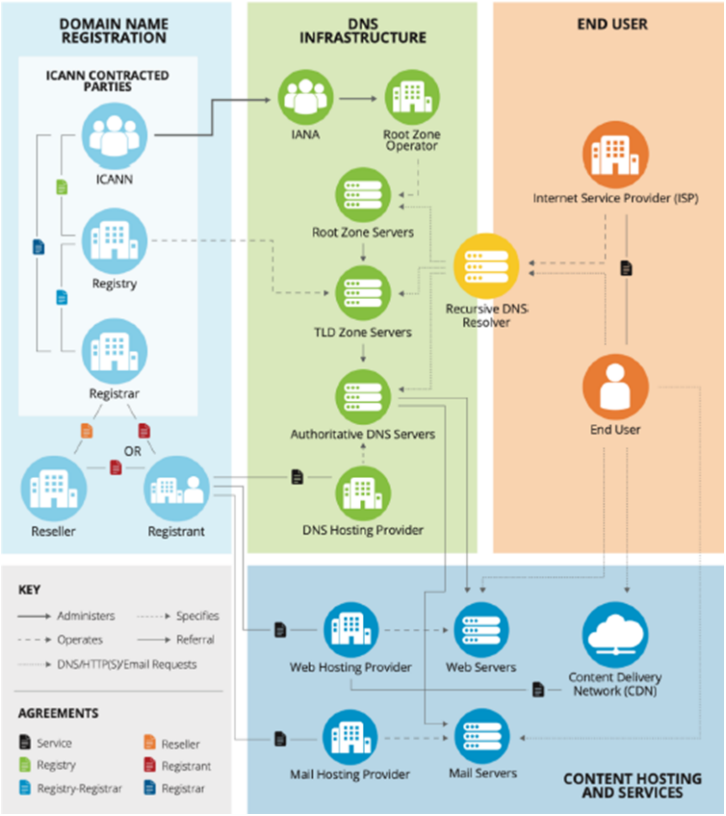


Figure 3.1: DNS Ecosystem Contractually Related to ICANN (image courtesy of Verisign and originally published in SSAC 115 adapted from [3])

3.3 Technological Advancements

Mitigation of DNS abuse is increasingly influenced by the integration of artificial intelligence (AI) and machine learning technologies [61]. At the helm of this evolution are innovative tools such as the iQ Domain Risk Score, which uses machine learning and string analytics to actively detect potential domain abuses now of registration [62]. This tool aims to act as an advance in the mitigation mechanism that prevents abuse by analysing the domains against criteria that indicate malicious intent in an attempt to stop the abuse before it takes place. The field sits at a crossroads of transformation in analysing evidence from abuse reports through the adoption of Large Language Models (LLMs), such as Generative Pre-trained Transformers (GPTs). The models are especially suited to parse and comprehend the complicated data relations humans may overlook, boosting the efficacy and automation of DNS abuse remediation and expanding the shield against cyber attacks. However, this progress also highlights an emerging challenge: the potential for malicious entities to exploit AI technologies themselves [63]. Therefore, the combination of AI and machine learning with DNS abuse mitigation marks an unprecedented milestone in the history of cybersecurity, while simultaneously serving as a warning that these technologies should not be used for harmful purposes. The present stage in the life cycle of DNS abuse is a time to reinvent and adjust more if digital ecosystems are to be properly protected.

3.3.1 Role of AI & ML

The introduction of AI and ML technologies into DNS abuse mitigation represents the dawn of an exciting new age of proactive detection and neutralisation of cyberspace threats [64]. The application of this technology makes it possible to quickly analyse large volumes of data and identify patterns that suggest an element of DNS query malevolence. For example, machine learning has been widely used in the analysis of DNS queries to categorise domain names. Based on the findings, it has become possible to detect malicious ones with a significantly higher level of precision [65]. For example, Li argued that machine learning reduced the number of false positives during domain verification. Meanwhile, neural network models, including the Extreme Learning Machine, exposed a level of precision of 99.5% while analysing malicious domain patterns. Thus, it has been shown that it is possible to increase the predictive power of AI in terms of cybersecurity [66]. Furthermore, DNS graph mining has shown the way of AI application possibilities in the domain of cybersecurity, such as the opportunity to exploit belief propagation algorithms allowing for high rates of precision for infected hosts and malicious domain identification. The following cases demonstrate the importance of AI and ML in DNS abuse, creating a new opportunity for rapid identification and early prevention. However, the complexity of AI models with an urgent need for transparency presents a significant problem. Although AI incorporation can contribute to secure measures against DNS abuse, the effort should not exclude ethics and certain governance considerations. Antonakakis et al. mention that "including AI in DNS abuse strategies will require consideration of the governance and ethics of stakeholders" [67]. 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 to build trust and ensures that people are responsible for them. There are difficulties in making things clear, such as the need to write down the data 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 transparency needed for blame.

In summary, AI and ML are useful for defending against a variety of devices and rapidly changing cyber threats, such as those in the IoT. The performance of their predictions is sometimes conditioned on the quality of the data and the volume of data used in the development of the system. Continuous learning and adjustment in AI/ML versions are essential due to the emergence of more advanced assaults which avoid detection algorithms.

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 [68].

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, making it dual-use in nature, both in normal operation and in a fallback communication channel [69]. The xHunt campaign [70] as seen in the figure 3.2 below 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 [71].

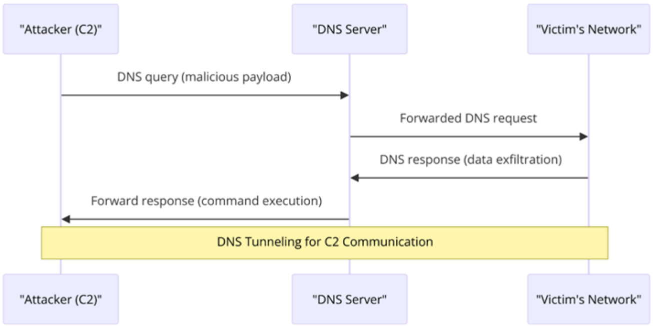

"Attacker (C2)"
"DNS Server"
"Victim's Network"
DNS query (malicious payload)
Forwarded DNS request
DNS response (data exfiltration)
Forward response (command execution)
DNS Tunneling for C2 Communication
"Attacker (C2)"
"DNS Server"
"Victim's Network"

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 [69]. The SUNBURST backdoor, as observed in Figure 3.3 below, 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 [72].

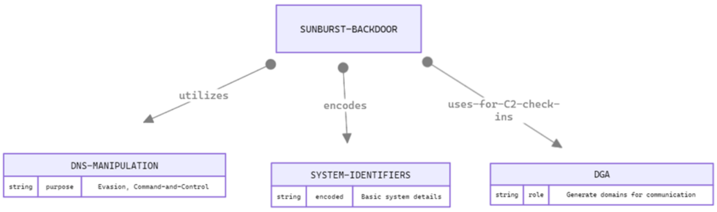


Figure 3.3: SUNBURST backdoor's utilization of DGAs and its associated components.

3. **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. [69].The major takeaway in the rapid rotation of IP addresses of this method, as the figure 3.4 below, points to the dynamism of strategies used in malicious communications, thus improving the means of defence by cybersecurity [73].

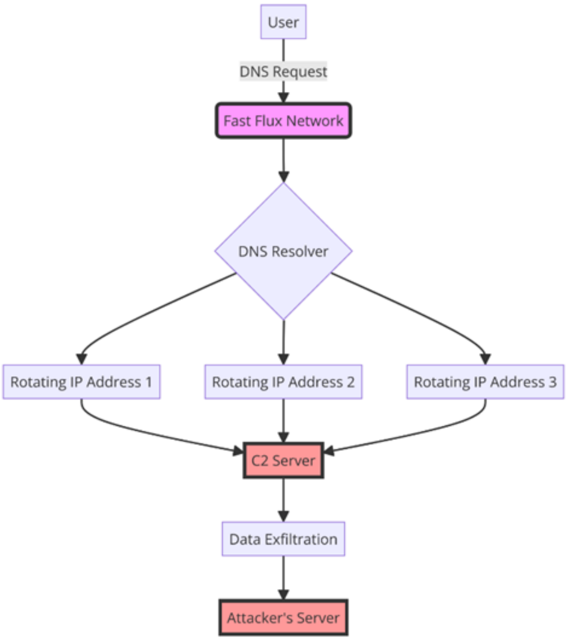


Figure 3.4: The usage of Fast Flux techniques by the Smoke Loader malware family for dynamic C2 domain communications.

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 as observed in the figure 3.5. From domains that mirror the information resources of COVID-19 to those that feign government relief programmes [69], the evolution of such attacks reflects a calculated approach to exploiting public interest and vulnerabilities [74] .

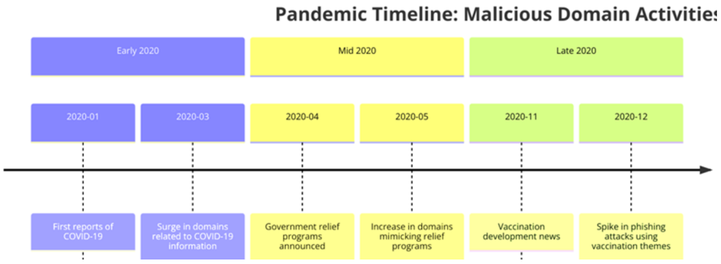

Pandemic Timeline: Malicious Domain Activitie:
Early 2020
Mid 2020
Late 2020
2020-01
2020-03
2020-04
2020-05
2020-11
2020-12
First reports of COVID-19
Surge in domains related to COVID-19 information
Government relief programs announced
Increase in domains mimicking relief programs
Vaccination development news
Spike in phishing attacks using vaccination themes

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 employed sophisticated tools, such as MFA pretending to 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 an 189% increase in attacks on pharmacies and hospitals from December last year to February this year. Advice was given to individuals and organisations that included 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, as figure 3.6 shows. Data have been normalised in such a way that the peak of each topic is 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.

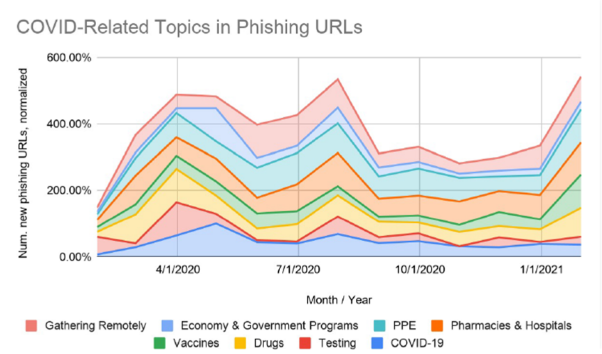


Figure 3.6: Development trends in the majority of COVID-19-related phishing content hosting sites during the period from January 2020 to February 2021. Adapted from [4].

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 as demonstrated in figure 3.7. 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.

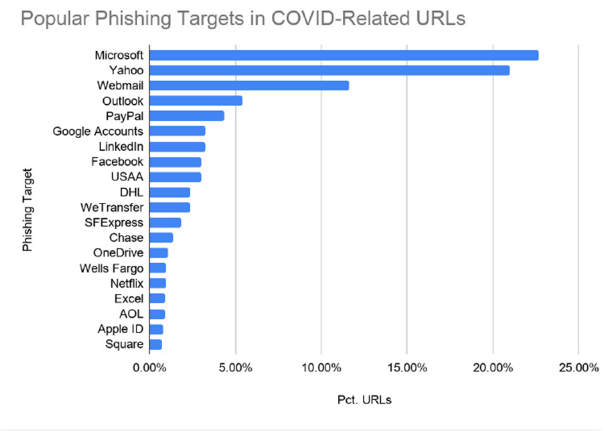


Figure 3.7: Top spoofed websites in COVID-themed phishing attacks (global), where the percentage in each column is the percentage of phishing volume per site and category. Adapted from [4].

Thus, this indicates a situation in which attackers frequently set up websites for COVID-19 themed phishing attacks as depicted in figure 3.8. Many of these phishing pages are found on sites created less than 32 days, meaning that these sites are launched for specific purposes because 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.

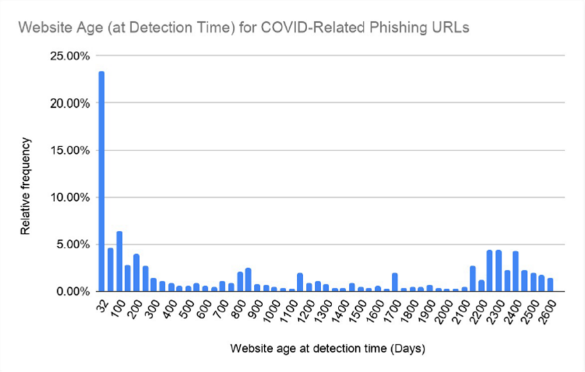


Figure 3.8: Statistic of lifespan distribution of COVID-19-related phishing content hosting sites when the sites are reported. Adapted from [4].

3.4.1 Identification of Current Challenges

Therefore, effective mitigation of DNS abuse requires the development of proactive measures that are continually updated in a way that adapts to the evolving landscape of cyber threats. Therefore, it is urgent to develop updated and evolving strategies with the evolving landscape. The cybersecurity sector needs to continue refining the tactics of the defence; otherwise, the bad actors will constantly refine their techniques to take advantage of DNS exposure. As for Internet and DNS abuses, since they transcend national frontiers, the only alternative to that serious problem is international cooperation. Now, the effectiveness of managing this kind of abuse would be through collaborative work between different nations, where experts in some geographical areas can come together and share their knowledge or resources [75]. Among the many challenges would be the jurisdictions' differences related to the legal and regulatory frameworks. Therefore, reaching a consensus position is difficult in the case of regulations, standards, or enforcement actions. The next challenge that arises is that both need to be reduced, and that would include reducing the number of false positives and negatives to check DNS abuse. One has to find a balance because overly strict measures can reduce user experiences, while too liberal can cause less activity detection. This is not good news for the cybersecurity community, which should be gearing up even further to protect people as these bad actors' tactics only grow in sophistication. This would enable maintaining security, meaning that the good healthy state of the integrity of the DNS system will remain a factor towards the protection of this Internet infrastructure.

3.4.2 Discussion on Future Research Directions and Technologies

ICANN77 showcased further developments related to the mitigation of DNS abuse, including the drafting of changes that would require registrars and registries to respond to abuse notifications. In a legal response by Freenom, global abuse levels decreased. The ccNSO Domain Abuse Steering Committee argued for a proactive mitigation strategy, but gNSO analysis finds that EU ccTLDs have a very low abusive rate and considers its possible reason to be market maturity and non-profit models [76]. Future activities will aim at building a new generation of tools with the help of new technologies, like artificial intelligence and machine learning, for enhanced domain security, to further support a larger global cooperation against shifting cyber threats. In other words, if better results are to be achieved, a high level of accuracy and wrong signals are not sent, more advanced AI and machine learning tools will be required, which will be able to understand the finer aspects of web traffic in detail [77].

3.5 Summary of Findings

Research on DNS abuse mitigation transparency points out how threats keep on changing, and therefore mitigation should also change. This is an indication of the value that community participation provides and the kind of transparency from which trust is built. Now, technological advancement is to be reviewed well, particularly in the field of AI and machine learning, to use for the detection of threats. Practical examples reflect the efficacy of various strategies. There is a balance between the introduction of new measures and the maintenance of effective teamwork and communication. Meanwhile, DNS abuse and subsequent staging should be effectively fought with a focus on such measures as technology, international cooperation, and standardisation of 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 collecting a wide range of 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 some of the 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 are most frequently encountered, with the aim of identifying 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 into understanding DNS abuse, as well as the mitigation of this abuse which provide a full view of current practices and potential areas for improvement with respect to the DNS ecosystem. The key themes and insights include:

- **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 and 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:** Responses include different strategies, from blocking orders from some regions to the use of software to monitor abusive activities. Recommendations were made in the area of education and outreach projects, such as NetBeacon and Compass, to report abuse and information on DNS abuse.
- **Role of Transparency:** Opinion on the transparency process was kind of mixed, since part of the respondents consider this positively because it is a tool that provides evidence to the industry in their fight against abuse and part of them consider negatively the way sensitive mitigation ways could be revealed. The consequence of transparency was elaborated on the development of relationships between all stakeholders, and there is, in general, a common understanding that transparency would increase understanding and teamwork through better communication on set measures against abuse.

Thus, the responses of stakeholders were quite valuable in providing a snapshot of practical challenges and possible mitigation strategies for DNS abuse. Consequently, it was a very valuable presentation of a real-world view of the need for the world to have adaptive definitions and comprehensive mitigation strategies, along with transparency in the ecosystem. This further extrapolates the theoretical knowledge with the help of the experiences of people involved on an active basis in the mitigation of DNS abuse.

4.3 Types of DNS Abuse Encountered

The stakeholder responses described the most common form of DNS abuse assumed within their area of interest. From these, views emerge for a variety of threats, where each of them brings unique challenges that favour specific mitigation measures.

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 in the pursuit of next-generation detection and response mechanisms.

4. Compromised CMS: Common encounters with the content management system (CMS) compromised. Consequently, attacks remain possible where some other existing vulnerabilities on web platforms are concerned. This kind of abuse is the reason why strong web security control practices should be in place and why platform operators must be alert.

5. "Water Torture" Attacks: Known as random subdomain attacks, they are even more technical and sophisticated ones. Such attacks not only compromise the regular functioning of DNS but also take some of the most sophisticated countermeasures to mitigate its impact on the affected parties.

The continued variation in DNS abuse experienced by stakeholders indicates that community efforts in terms of collaborations, innovations, and education will build on the experiences derived from stakeholders and inform the most relevant foundation on which effective strategies and policies will be developed to mitigate DNS abuse effectively.

4.4 Challenges in Mitigation and Mitigation Strategies

The responses of the 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 clear barrier related to the economic nature of the DNS industry was identified, which is characterised by low margins and high volumes, leaving little resources to help mitigate DNS abuse on a large scale. The responsible registrars stressed that 80% of the malicious domain name registrations were related to several large and reputable registrars and some small registrars, which is an example of how, from an economic point of view, the cost of security is not proportional to the amount of dangerous information that is being exploited. This points to a clear economic barrier in the DNS ecosystem and calls for new ways of efficient and economical mitigation.
2. Regulatory Gaps: The regulatory environment was mentioned as a challenge. Included poor, weak, or lack of policies and enforcement mechanisms that did not allow us to combat DNS abuse properly. Therefore, all respondents also emphasised the need for more clear regulations and standards that could better guide industry attempts to mitigate abuse.
3. Mitigation Strategies: They have focused on components of education, collaboration, and outreach to create knowledge and a social response. Software tools to support these efforts, abuse reporting intermediaries and measurement projects that measure the Internet, are crucial in finding, reporting, and understanding abuse cases. These tools are also designed to help report and mitigate risk, but can collect critical data with a policy and the character of a regulatory response.

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: Transparency is increasingly recognised as a method for sector participants to show a firm-wide commitment to combating DNS abuse. By allowing mitigation efforts to be driven down the stack and done more rapidly and often overtly, the action becomes associated with a culture of accountability and responsibility. However, when it comes to issuing data on the prevalence of abuse and the effects of mitigation measures, transparency can strengthen confidence among users, regulators, and sector participants. Furthermore, it is acknowledged as a

contributing element to a comprehensive understanding of and collaboration among the various actors in the DNS landscape. Operators, registrars, registries, and regulators may have a better understanding of the difficulties and achievements of many other performers in the section if they exchange data on abusive activities and mitigation measures.

2. Challenges and Concerns: Stakeholders raised several concerns about the degree and manner of transparency. One fear is that some sensitive mitigation strategies are being disclosed and could serve as a means for the bad guys to find ways to find out about abuse and its mitigation. Many within the industry find here a fine balance between useful information on the one hand and, at the same time, protecting operational integrity on the other. Additionally, there is apprehension that increased transparency could lead to regulatory or legal consequences, especially if disclosures are mandated in a manner that does not consider the practical aspects of abuse mitigation. Stakeholders also pointed out such operational challenges as the ability to complete transparency reporting, given the current reliance on less formal mechanisms to report abuse and monitoring mitigation.
3. Strategic Approach to Transparency: The stakeholders are for the vision that a strategic approach to transparency in support of the goals and aims for mitigation of DNS abuse should, in no way, be undermined from being effective. This would include targeted transparency, with the point being more aggregated data and trends than detailed disclosure of specific mitigation actions or techniques. But this environment should be nourished where sharing information does not result in punitive consequences, but, on the other side, supports collaborative improvement, which is considered essential. The value of transparency for the mitigation of DNS abuse is considered of high value, but stakeholders advise to be careful with each step in what, how and to whom it will be disclosed. This shall be a balanced approach that increases the collective ability to address DNS abuse, rather than safeguarding methods used. In short, it is of the utmost importance for the continual 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 following is a summary of the emailed responses of the stakeholders in relation to DNS abuse mitigation. 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 is 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

When analysing the data from the stakeholder responses, a thorough examination of DNS abuse was carried out. The stakeholders provided valuable information on the definitions of DNS abuse. The commonly mentioned type was phishing due to its spectrum in all aspects, compromised CMS, and confusables were also identified by everyone as prevalent. The most challenging aspects of mitigation included economic factors that influence achievable levels of DNS abuse in the branch and regulatory gaps because the market structure changes the evaluation of mitigation abuse measures and the lack of set regulations blurs perceptions. The mitigation strategies and plans implemented are based on targeted blocking and collaborative education; their efficiency is reduced by the industry's focus on performance and the paths of different entities. Transparency is described as a double-sided weapon; although it has accountability and trust-building potential, it can harm the industry when people use their malicious understandings. Stakeholder experiences and actions contribute to the understanding of DNS abuse, maximising the need for a multidimensional approach based on adaptation, cooperation, and the equivalence of transparency.

5 Implementation

This chapter focuses on the practical implementation of the Domain Legitimacy Checker. The multiviewed approach, along with programming in Python and the web framework in Flask, HTML, CSS, and JavaScript, on the side of external APIs, greatly assisted in making a simple framework for DNS abuse detection and transparency improvement. With these alternatives, a simple but effective method has been developed for determining the legitimacy of domain names, but also for showing clearly the various tactics which bad actors are using in the adoption of confusable domains for phishing and malware distribution, along with other malicious activities to aid with my research. This effort embarked on a journey from idea to execution, focussing on a user-friendly web interface that allows users to quickly identify potentially malicious domains. For further details, refer to the program code listed in the appendix A1.3.

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 detailed check, the system queries external APIs such as VirusTotal for additional legitimacy checks. The results of such checks 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.

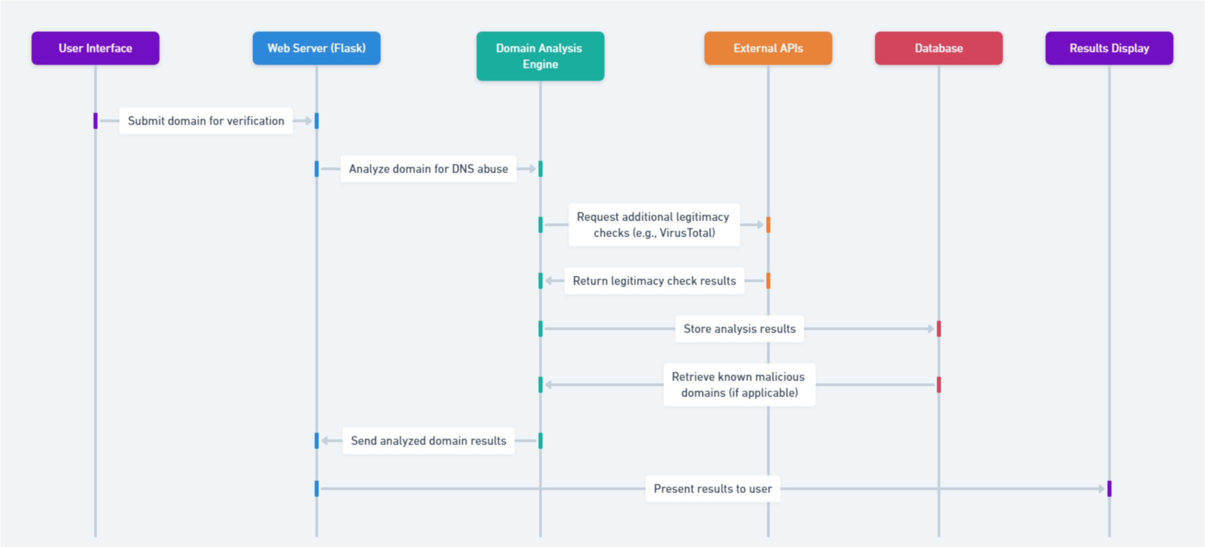

User Interface
Web Server (Flask)
Domain Analysis Engine
External APIs
Database
Results Display
Submit domain for verification
Analyze domain for DNS abuse
Request additional legitimacy checks (e.g., VirusTotal)
Return legitimacy check results
Store analysis results
Retrieve known malicious domains (if applicable)
Send analyzed domain results
Present results to user

Figure 5.1: Domain Legitimacy Checker

5.2 Tools & Technologies

The domain legitimacy checker shown in figure 5.2 was built using Python with the use of its third-party modules for development and to provide ways of 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 is empowered by CSS3 for styling while allowing Bootstrap for a 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. Request libraries also connect to external APIs such as 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 to host phishing sites, distribute malware or participate in suspicious activity should be filtered. The choice of each of the tools and technology used was based on its merits but on their integration, making sure that all the systems combined to achieve the cohesiveness and effectiveness of detecting DNS abuse and transparency.

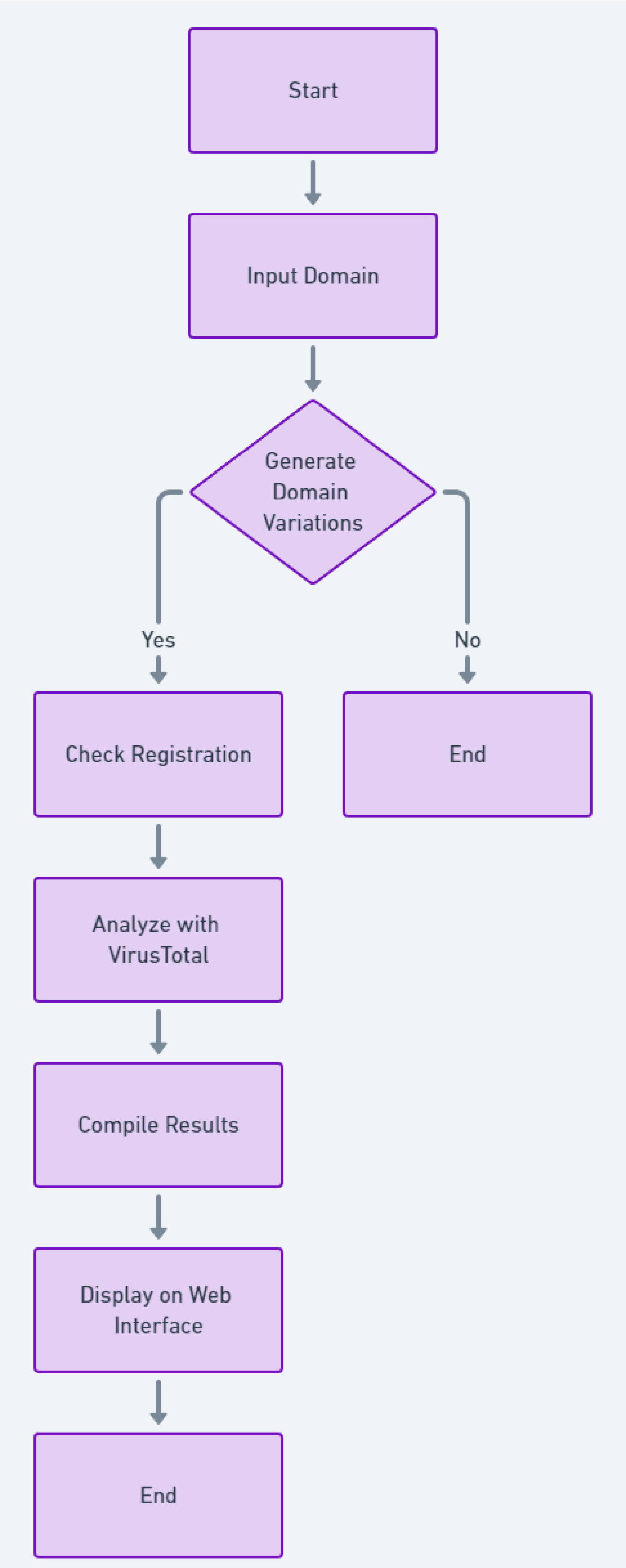
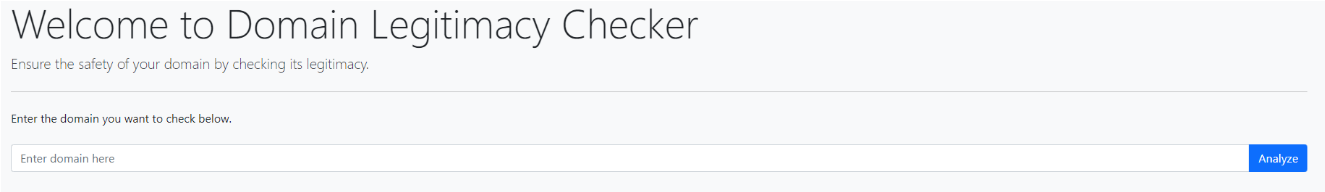


Figure 5.2: Domain Legitimacy Checker

5.3 Visualisations

The interface and layout of the web page, as shown in 5.3, have been designed to facilitate and smooth transition with users. The interface was specially designed so that 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 jumps 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.



Welcome to Domain Legitimacy Checker

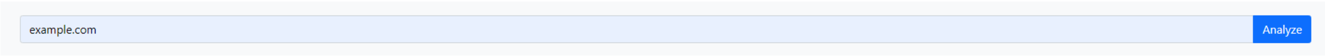
Ensure the safety of your domain by checking its legitimacy.

Enter the domain you want to check below.

Figure 5.3: The main interface of the Domain Legitimacy Checker

5.3.1 Input & Interaction

The Domain Legitimacy Checker Tool provides a place for interaction with users to ensure a seamless experience, as you can see in 5.4. The domain input method, a single-field form designed for simplicity of use and quick analysis, is at the centre of this interaction.



example.com

Figure 5.4: 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. Right next to the text box is the "Analyze" button as depicted in 5.5, contrasting with blue to stand out visually and identify 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.

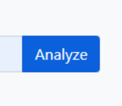


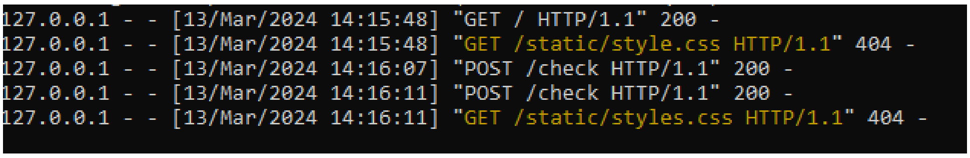
Figure 5.5: The 'Analyze' button, poised for user action after domain entry.

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.

5.3.2 Interactive Features

The program comes with an interactive interface; the user is engaged in all the steps from entering a domain for analysis to receiving the results. Starting from the second user having submitted 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 cookie is returned to signify a successful search. Such types of interaction are logged as entries in the server log, forming a very critical and highly detailed timeline of activities. Figure 5.6 below visually summarises this process.



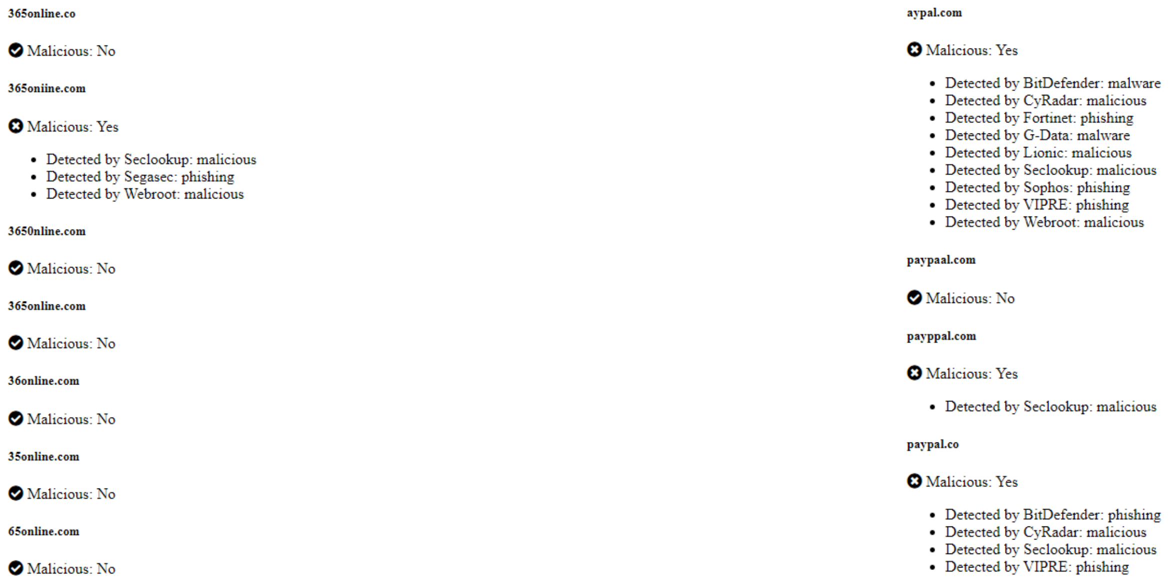
```
127.0.0.1 - - [13/Mar/2024 14:15:48] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [13/Mar/2024 14:15:48] "GET /static/style.css HTTP/1.1" 404 -
127.0.0.1 - - [13/Mar/2024 14:16:07] "POST /check HTTP/1.1" 200 -
127.0.0.1 - - [13/Mar/2024 14:16:11] "POST /check HTTP/1.1" 200 -
127.0.0.1 - - [13/Mar/2024 14:16:11]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

Figure 5.6: Server log entries capturing real-time HTTP requests and responses

If there is any issue, these logs are important, for example, in the case of a "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.

5.3.3 Results Display

The Domain Legitimacy Checker displays the findings in an easy-to-understand style after 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 check mark 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 figure 5.7 and clearly show how the program works when domain names are checked.



365online.co

✓ Malicious: No

365oniine.com

✗ Malicious: Yes

- Detected by Seclookup: malicious
- Detected by Segasec: phishing
- Detected by Webroot: malicious

3650nline.com

✓ Malicious: No

365online.com

✓ Malicious: No

36online.com

✓ Malicious: No

35online.com

✓ Malicious: No

65online.com

✓ Malicious: No

aypal.com

✗ Malicious: Yes

- Detected by BitDefender: malware
- Detected by CyRadar: malicious
- Detected by Fortinet: phishing
- Detected by G-Data: malware
- Detected by Lionic: malicious
- Detected by Seclookup: malicious
- Detected by Sophos: phishing
- Detected by VIPRE: phishing
- Detected by Webroot: malicious

paypaal.com

✓ Malicious: No

payppal.com

✗ Malicious: Yes

- Detected by Seclookup: malicious

paypal.co

✗ Malicious: Yes

- Detected by BitDefender: phishing
- Detected by CyRadar: malicious
- Detected by Seclookup: malicious
- Detected by VIPRE: phishing

Figure 5.7: visual indicators showing the legitimacy status of analysed domains.

For the malicious domains identified above, the interface unfolds more information as an itemisation of the security threats detected. In each domain, the scanner's findings indicate the exact categories of malicious activities the scanners were able to detect, including malware, phishing, or other security issues. These details are not only comprehensive but also indicate to the user what might be looked for as the next mitigation step or further investigation. In basic terms, an online brand with such recognition and worldwide users, PayPal is more likely to enter into phishing exploits and use confusable domains compared to the local brand: Bank of Ireland. In this context, although the Bank of Ireland essentially has a local-based client, PayPal does an international scale of operation with huge numbers of clients using their services. Usually, it is a rule that most domain names registered by bad actors closely resemble the official PayPal ones to phish sensitive information from the users. This higher risk factor is directly related to the prominence and wide-reaching scope of PayPal, vis-à-vis a more geographically confined and less known Bank of Ireland.

5.3.4 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 as shown in figure 5.8. It normally does this through a button that shows on the interface for this function and that simply says "Check Another Domain." This reconnects the user with the input interface.

Check Another Domain

Figure 5.8: The 'Check Another Domain' button

This iterative process is another characteristic of the user, 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.

5.4 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 virus total rate limit API is a very common rate. It is now going to be a problem because it has a limited number of requests and if they exceed that set number, then the service will be temporarily blocked.

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 important to give 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.in principle for network operations.

Solution: Pass the data to the servers and receive its result from the servers without refreshing the web page using JavaScript.

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

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

5.5 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; the Python unit test framework was used. The mock objects were used to simulate the acts of external APIs.Manual and automated tests were performed in front-end technologies. Automated UI tests, such as those with Selenium, were used 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 were 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, the focus will be on evaluating and discussing the project and, most importantly, two forms of DNS abuse, which are confusable domains and phishing due to their popularity among bad actors by testing and validating them. The chapter 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 the project met the objectives. In addition, a proposal will be made to improve the transparency around these mitigation strategies to foster accountability and trust. Through the analysis, the feasibility of implementing such transparency measures will be assessed by performing an analysis using data and evidence. Finally, the limitations of the work will be addressed.

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.

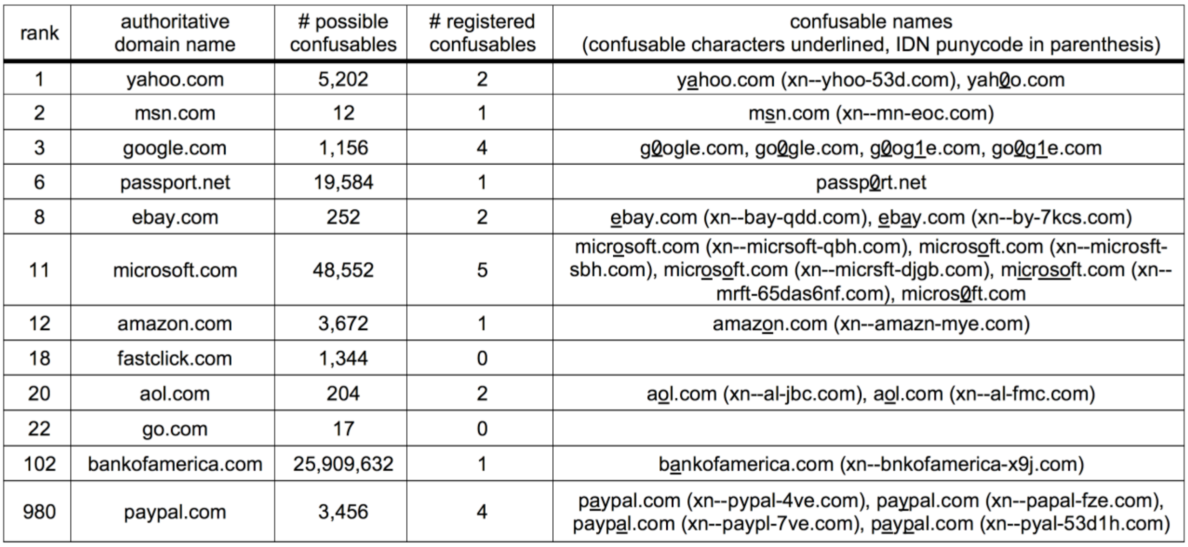
- **Commercial Appeal:** The domains with commercial appeal attract traffic and can generate income. They are short and memorable and relate to popular products or services, sometimes leading to ownership arguments [78].
- **Keyword Relevance:** Similarly, a domain specific to keywords ranks well in 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 :** A famous case was of Amul in 2019-2020. The renowned dairy giant had an impersonation case of similar domain registration, which was used to lead the public toward phishing, such as for fake distributorship or job opportunities. The Indian dairy brand above had this issue repeated three times in the last three years, namely from 2018 to 2020, and the company had to publish public notice while sending legal bodies, which also exhibited to readers the extent to which one can go for the brand defence issue.[79].
- **Typosquatting :** 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 [80].
- **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 [81]. 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 [82].

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. "paypaI.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" [83], 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. Figure 6.1 clearly shows, 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 implemented to protect Internet users from such deceptive practices.



rank	authoritative domain name	# possible confusables	# registered confusables	confusable names (confusable characters underlined, IDN punycode in parenthesis)
1	yahoo.com	5,202	2	yahoo.com (xn--yhoo-53d.com), yah0o.com
2	msn.com	12	1	msn.com (xn--mn-eoc.com)
3	google.com	1,156	4	g0ogle.com, go0gle.com, g0og1e.com, go0g1e.com
6	passport.net	19,584	1	passp0rt.net
8	ebay.com	252	2	ebay.com (xn--bay-qdd.com), ebay.com (xn--by-7kcs.com)
11	microsoft.com	48,552	5	microsoft.com (xn--micrsoft-qbh.com), microsoft.com (xn--microsft-sbh.com), microsoft.com (xn--micrsft-djgb.com), microsoft.com (xn--mrft-65das6nf.com), micros0ft.com
12	amazon.com	3,672	1	amazon.com (xn--amazn-mye.com)
18	fastclick.com	1,344	0	
20	aol.com	204	2	aol.com (xn--al-jbc.com), aol.com (xn--al-fmc.com)
22	go.com	17	0	
102	bankofamerica.com	25,909,632	1	bankofamerica.com (xn--bnkofamerica-x9j.com)
980	paypal.com	3,456	4	paypal.com (xn--pypal-4ve.com), paypal.com (xn--papal-fze.com), paypal.com (xn--paypl-7ve.com), paypal.com (xn--pyal-53d1h.com)

Figure 6.1: confusables registered for popular domains, adapted from [5].

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 [84]. 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 [85].

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). The threat of these two groups is vastly different and the technical possibility of most mitigation strategies also varies greatly. The subsequent section of the paper describes the mitigation methods in detail, addressing their operational feasibility and potential collaboration initiatives.

Non-IDNs Mitigation Techniques: These techniques aim to detect and mitigate domain squatting and typosquatting, where the attacker registers a typographical error or variant of a legitimate domain so that users get confused.

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 [86].
2. Trademark Protection Programmes: Trademark Clearinghouse (TMCH) offers mechanisms for trademark owners to protect their rights by receiving notifications when someone attempts to register a domain that matches their trademark [87].
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 [88].

IDNs Mitigation Techniques: The problem with IDNs is the potential for homograph attacks, where attackers can use characters from different scripts that visually appear to look like characters in Latin script.

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 [89].

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 [90].
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 [91].

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 malicious 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 their 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 DNStwist 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; It will mainly require the use of existing technology and cooperation that could be initiated with little difficulty between stakeholders.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. Registry-Level Measures: Not Feasible; this would require very heavy coordination and agreement on standards across diverse jurisdictions and registries.

6.2 Phishing

6.2.1 Real-life examples

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 [92] .

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-changing cyber threats [93].

6.2.2 Real-life Mitigations

- **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 [94].
- **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 [94].
- **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 [95].

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 [96].

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 idea of a detailed thinking process of the offender, along with the description of the attributes in the environment that allow the attack to occur, is introduced with the Situational Crime Prevention Approach [96]: This method was developed considering the theory that it is possible to deter potential attackers if the level of effort they make, the risk they take, and the likely rewards they receive are raised, stay the same, and lowered accordingly. It is worth mentioning that the criminal perspective is necessary to understand, and creating a hostile environment for phishing operations by implementing certain strategic preventive measures is crucial. This method includes the following steps:

1. Increasing the Effort for Attackers: Implement strong authentication mechanisms and encryption to increase the difficulty of accessing or spoofing phishing websites or legitimate email accounts.

2. Clarifying User Responsibilities: Information about users' role in security, such as awareness of phishing signs and reporting aids.

3. Enhancing Detection Probability: Using the latest detection technologies and threat intelligence to recognise and eliminate phishing threats on time.

4. Limiting Phishers' Access: Limiting the breadth of information that is accessible to the public, which might be used to construct compelling phishing emails and fake the identity of someone else or an organisation.

5. Discouraging Future Attacks: Implement punitive actions such as tracking down familiar attackers and sharing information about the attack with a larger group of people to deter 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. 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 [97] , 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): Examines the network packet data more than the basic header information. Used to look at the content of packets looking for known

signatures and patterns associated with phishing.

2. Store and Forward (SF) and Forward and Inspect (FI) modes: SF mode temporarily stores packets for a thorough inspection before forwarding, while FI mode prioritises immediate forwarding with a parallel inspection to reduce latency.
3. Artificial Neural Network (ANN): A machine learning model used to classify network traffic based on characteristics to detect links to potential phishing signatures.
4. Dynamic adjustment of network flows: In the case of standard recognition, the system can dynamically change the routing to bypass the link or reduce flow to prevent the phishing process.
5. Minimal disruption to network services: Designed to maintain the mitigation process minimised without targeting performance to ensure that final services would run smoothly even during the measure.

6.2.4 Transparency in Mitigation Efforts

Here is how transparency can be applied to each of the mitigation techniques described:

- **Employee Awareness and Training :**

  Communication: This will consist of clearly informing the employees about the kind of threat and what 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.

- **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 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 of reporting unlisted phishing sites and correcting false positives by stakeholders.

- **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, therefore, they make efforts to reduce it.

- **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.

6.2.5 Analysis : Feasibility & Practical Challenges

1. Comprehensive Security Measures :Feasible; The deployment of web filters and secure browsing policies is technically straightforward with existing technology. The main effort lies in the continuous update of policies and employee education.
2. 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.
3. Awareness against unsolicited emails: Feasible; Establishing and communicating best practices for handling suspicious emails involves minimal costs and leverages existing communication channels within organisations.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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 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 together 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 [98]. To put this into perspective, here are some examples:

1. New specifications on defining DNS abuse have been entered into ICANN's contracts from ICANN's contracted parties. Furthermore, there are clear requirements that define the actions to be taken by registry and registry after receiving immediate actionable evidence of abuse. This move clarifies the roles that different stakeholders can play in addressing the DNS abuse issue and establishing a common approach to redress [99].

2. Some of these new duties have been positively approved by the community. The community supported the new obligations of the ICANN contract parties to further mitigate DNS abuse. The message that this example sends to everyone is that the community is willing to join and participate in DNS abuse and other challenges to address [100].

3. Efforts such as 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 registrars, ultimately narrowing down their scope to the relevant and evidenced report, and 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 [101].

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. Consider the following:

1. Governmental Efforts to Block DNS Resolutions: Governments may interfere directly with DNS operations 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 [102].
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 areflagged, 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 [103].
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 [104].

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

At the same time, the issue of publishing confusable domain lists, while ultimately beneficial for cybersecurity, also implies several limitations and security issues, such as the problem of phishing. First, the reason for concern is that publishing these lists can serve as a manual for bad actors since it potentially discloses potential domains for phishing. For example, if victims are exposed in such a way, bad actors can quickly adjust their approaches, ensuring that their activities stay one step ahead of countermeasures. Second, false positives, or legitimate domains that are mistakenly identified as confusable, also represent a serious challenge. For real businesses and people, a loophole for that is their potential association with phishing since this can entail unnecessary attention, legal action, and reputation damage. Third, the issue of transparency also raises concern about how relevant releasing such data is in terms of attack prevention. While the logic of making the lists available to the public before they can be misused for abuse, such as phishing, is clear, the sheer volume of domain registration and the continuous changes in domain abuse tactics undermine their actual usefulness for end-users and organisations to proactively identify and tackle phishing risks.

6.6 Limitations of Research Conducted on DNS Abuse Transparency

1. Variability in reporting standards: The majority of challenges faced in actual practice come with a lack of uniformity in standards from DNS infrastructure providers from the definition of abuse to the thresholds of actions and how those actions are being reported. This inconsistency has made efforts to collect and compare the data of different entities difficult to piece together into one coherent picture for sensible enforcement of DNS abuse mitigation.

2. Limited Availability of Data: The general lack of transparency reports that are available to the public. Providers either do not at all release or do, and in doing so,

have an omission of information required to be looked into. This means that there are still gaps in understanding the whole spectrum of strategies deployed by the DNS abuse domain due to data unavailability.

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 tend 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: Due to the specific nature of the Internet ecosystem, it is quite challenging to evaluate the efficacy of DNS abuse mitigation techniques. Furthermore, the evaluation process is quite complex due to the indirect impact of specific actions of DNS abuse prevention efforts on the larger effects.
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.

As demonstrated, all these limitations show the complex difficulties in conducting a thorough research on DNS abuse mitigation transparency. Only by operating with the principles of team interaction, originality, and a willingness to develop research tools and approaches in the given area, can the misrepresentation difficulties be resolved.

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 objective of these projects was to increase the understanding and transparency of stakeholders about reporting DNS abuse. Despite many challenges that the project faced, such as working with different reporting standards or limited access to data, this effort managed to uncover light flaws in the approach to mitigating and reporting DNS abuse. This project also demonstrated the high level of complexity and variety of approaches taken by different institutions in reporting, which accentuated the importance of unified and mandatory reporting requirements.

6.7.2 Impact on Understanding DNS Abuse

Given the difficulties, the research project yielded valuable information on the state of mitigation of DNS abuse. It showed that DNS abuse is unpredictable and, due to rapidly changing tactics of bad actors, mitigation measures should also be updated regularly. The study revealed several gaps in current knowledge and approaches to address, as shown by the lack of transparency reports and the unwillingness of providers to share critical data on their scopes. These findings could lay the ground for further research and policy-making.

6.7.3 Stakeholder Engagement

It was important to include interaction with stakeholders, including registry owners, policy makers, and DNS registry. The project encouraged discussion of the need for increased sector and jurisdiction cooperation and transparency. However, it seems that there is more to be desired in the impact on stakeholder behaviours and policies: for example, more proactive efforts and collaboration in the fight against DNS abuse.

6.7.4 Practical Implications

The outcomes of the project lead to positive results in the impact of transparency in reducing DNS abuse. Implementing recommendations for setting up standardised report creation processes and facilitation of data exchange could lead to more coherent and effective DNS abuse mitigation efforts. These recommendations provide practical next steps for stakeholders to better address the issues raised.

6.7.5 Suggestions for Improvement

Future projects, therefore, can discuss study questions on newly developed strategies, which abuse DNS, and research more aspects of transparency, so that they can obtain deeper insights. Further improvements in how to engage stakeholders include more transparency in forums to work with them toward the establishment of joint research projects, thereby increasing the scope and quality of information. 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. This development would represent a significant step forward in creating greater transparency and consistency in efforts to mitigate DNS abuse in recognition of the work being done and research and cooperation that will continue. Consequently, the way forward demands that all actors work together toward the recommendations for having a more secure, safe online environment.

7 Conclusion

7.1 Brief Review

This project has looked at the abuse of the DNS, in which a situation leads to malicious actors using domain names for their malicious activities, such as phishing. DNS infrastructure providers, including registries and registrars, have thus focused on playing a role in controlling, if not reducing, this abuse. The research included complaints received from providers and steps taken to abuse by deleting or blocking name registrations. Therefore, the core of the study lies in the concept of transparency and the degree to which providers disclose and document these actions. Obviously, the issuing of comprehensive transparency reports does not go as far as the requirement, and it is a very key aspect towards promoting trust and accountability in the digital world.

7.2 Main Results

7.2.1 Related back to Project Objectives:

This project led to the serious transparency gaps in the mitigation of DNS abuse adopted by infrastructure providers. Mitigation action against DNS abuse includes technical measures, such as the traceability of responsible individuals and strict reporting and communication of mitigation action. This goes parallel with our first objective: to understand how the area practices on transparency and, when necessary, establish a requirement for standardised measures.

7.2.2 Summary of Proposals:

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

1. Regular Transparency Reporting: Ask DNS infrastructure providers to provide information to the public regularly about the actions they have taken in their fight to mitigate against DNS abuse.

2. Stakeholder Engagement: Increase cooperation and communication to regulate transparency between DNS providers, users, and legislators. .
3. Public Accountability Mechanisms: Members of the general public should have ways through which they can monitor and evaluate DNS efforts to mitigate abuse.
4. Innovation in Defence Strategies and Sharing: Create a framework that indicates the development of strategies to enable one to be ready and share the strategies among the participants to enhance innovation in their efforts in the fight to end different abuses.
5. Transparency in Monitoring and Collective Action: Open observation of DNS activity and the collective participation of all parties in the DNS ecosystem to work towards a single approach to end the abuses.

These strategies try to supplement the fundamental measures of the research project already listed by also taking into account the providers of the efforts of the DNS infrastructure, as well as the efforts and shared responsibilities over the DNS ecosystem. The Internet community can achieve a much more reliable system by enhancing the level of trust and transparency, thus enforcing a DNS system that protects against abuse more effectively.

7.3 Future Work

7.3.1 Further Research Directions:

Future research needs to work towards integrating AI and machine learning in predictive DNS abuse detection, as well as the extent to which international regulatory frameworks manage to establish transparency requirements. This could be further researched into how the difference in degrees of openness and transparency changes user trust and behaviour, in addition to transparency, and the perception of infrastructure DNS providers. 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: Develop a common transparency framework that could be adopted by DNS infrastructure providers around the world and work closely with the respective leading industry partners on this matter.

2. Technology Solutions: Explore technical mechanisms for automating the transparent collection and dissemination of DNS abuse data.
3. Policy recommendations: The requirement of transparency in those activities should be a prerequisite for the formulation of policies and incentives for legislative support for DNS abuse mitigation efforts.
4. Stakeholder Collaboration: Regulatory bodies responsible for maintaining DNS infrastructure and cybersecurity communities unite their efforts to fight and find a solution to these issues.
5. Transparency standardisation: Industry-wide standardisation of the reporting process would go a long way to maintaining a healthy level of uniformity in the matters of disclosure regarding behavioural efforts when addressing DNS abuse.
6. Real-Time Monitoring: Ensures timely detection and response to threats and utilisation of real-time dashboards
7. Public Awareness: User education on DNS security can boost the general public's knowledge of the subjects, thereby protecting them from 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: Issue a comprehensive and consistent transparency report that includes the number of abuse reports received, the actions they recommend, and the follow-up action on them. Moreover, transparency builds trust among users and holds the organisation accountable for efficient abuse mitigation.
2. Stakeholder Engagement: Create forums or advisory boards to discuss and assess DNS solutions to mitigate abuse. This should involve a broader selection of stakeholders, including government officials, cyber security specialists, and representatives of civil society. This can help guide the decision-making process with input from all sides.
3. Best Practice Sharing: Encourage a transparent environment by sharing best practices, resources, and innovations to mitigate DNS abuse with colleagues in the DNS ecosystem.
4. User Education: Recreate and share educational materials to assist domain owners and end users in recognising and avoiding DNS abuse. When people are well informed,

they become intelligent for most abuses.

5. 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: Research DNS, the abuse that may arise and build a solution-targeted mitigation around AI-generated content and the growth in IoT devices.
2. AI and Machine Learning for Proactive Defence: Data analysis to identify possible abuse trends and support AI and machine learning solutions that can anticipate and address DNS abuse before it occurs.
3. Enhanced IoT Security: advocates for the spread of security measures through partnerships and laws for manufacturers of IoT devices to hopefully change the fact that IoT devices have a homogeneous trigger and seek a tendency from which an abuser can attack a device.
4. Global Policy and Regulation Dialogue: Engage in policy discussion and implementing Database Coordination and laws that can bring growth and satisfy cyber infrastructure security, privacy, and freedom.
5. Transparency Evolution: Evolution of transparency in line with evolving tech, consider setting up real-time data sharing, blockchain log reporting, and user-friendly setups to deter unauthorised access to data.

7.3.5 Contributions to Future Transparency Practices:

This research further contributes to the ongoing development of best-practice for transparency in reporting on DNS abuse mitigation. This emphasises the importance of transparent and consistent reporting and interaction with stakeholders so that policy makers can rely on reporting for informed policy formulation and to be able to contribute to safer cyberspace. Therefore, this has been one of the main findings of this study in the remaining challenges of the field. The ways out include informed and active user bases, reduction of DNS abuse, and even more reliable Internet ecosystems.

7.4 Reflection

7.4.1 Personal Learning:

This project really opened my eyes and taught me a lot about the complexity of DNS abuse and how this could pose a challenge in the development of systems due to the potential lack of transparency. DNS abuse can be viewed as dynamic, in the sense that it continues to evolve to show new tactics used by the bad actors, so that the mitigation strategies also need to be adaptive. And what I have learnt is that transparency in work is not only sharing information, but, in fact, it helps build trust within the community, increases efficiency of efforts aimed at abuse mitigation, and has an overall positive influence on governance of the Internet and security.

7.4.2 Evaluation of Research Process:

In other words, this research project exposed serious challenges to the study of transparency in mitigating DNS abuse, from secrecy in sharing sensitive data, dreaded by privacy and security considerations, to the threat of data self-reporting biases. What it made clear was the fact that the process made it clear that a delicate balance needs to be achieved between the need for security and releasing just enough information to be, basically, transparent. However, these approaches allowed in-depth research to be carried out, and at the same time, they criticised the general area of what needs to be improved, including methods to identify more accurate ways by which transparency practices influence the reduction of DNS abuse.

7.4.3 Perspective on Research Findings and Contributions:

This research project provides a broader look at current practices and how effective they are within the ongoing discussions on how to mitigate and possibly even yield more effective transparency of DNS abuse. This research suggests that there should be an organised approach to openness from gap analysis and practical strategy recommendations. This calls for designing best-practice guidelines that strengthen cooperation among all the parties in the DNS ecosystem. Although very good progress is being made, my work highlights the continued need for attention and effort in this area, suggesting that the road toward a more transparent, safe, and abuse-resistant DNS landscape is very far from complete.

This project has broadly enriched my knowledge in relation to mitigation of DNS abuse and transparency pursued, while provoking very important information that should take this field into account in future research in the area of cybersecurity and Internet governance.

Bibliography

[1] C. Blanche. (2018) Understanding dns. Accessed:28/03/2024. [Online]. Available: https://chrisblanche.com/2018/08/11/understanding-dns/

[2] M. S. Rich, "Cyberpsychology: A longitudinal analysis of cyber adversarial tactics and techniques," *Analytics*, vol. 2, no. 3, pp. 618–655, 2023, accessed:04/04/2024. [Online]. Available: https://www.mdpi.com/2813-2203/2/3/35

[3] Security and Stability Advisory Committee, "Title of the report," ICANN, SAC Series 115, 2023, accessed:28/03/2024. [Online]. Available: https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-115-en.pdf

[4] L. Hu. (2021) Fake websites used in covid-19 themed phishing attacks, impersonating brands like pfizer and biontech. Accessed:28/03/2024. [Online]. Available: https://unit42.paloaltonetworks.com/covid-19-themed-phishing-attacks/

[5] S. Gajek, J. Schwenk, L. Feldmann, and M. Jensen, "Cutting through the confusion: A measurement study of homograph attacks," in *Proceedings of the 15th International Conference on World Wide Web*. ACM, 2006, pp. 393–402, accessed:25/03/2024.

[6] J. So *et al.*, "Domains do change their spots: Quantifying potential abuse of residual trust," 2022, accessed: 25/10/2023. [Online]. Available: https://ieeexplore.ieee.org/document/9833609

[7] J. Bayer *et al.*, "Study on domain name system (dns) abuse: Technical report," 2022, accessed: 25/10/2023. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/d9804355-7f22-11ec-8c40-01aa75ed71a1/language-en

[8] C. Hesselman, P. Grosso, R. Holz, F. Kuipers, J. H. Xue, M. Jonker, and C. D. Laat, "A responsible internet to increase trust in the digital world," *Journal of Network and Systems Management*, vol. 28, no. 4, pp. 882–928, 2020, accessed: 25/10/2023. [Online]. Available: https://link.springer.com/content/pdf/10.1007/s10922-020-09564-7.pdf

[9] A. Mathew and C. Cheshire, "Trust and community in the practice of network security," 2016, accessed: 25/10/2023.

[10] V. Cerf, "Preserving the internet," *Communications of the ACM*, vol. 65, no. 4, pp. 6–7, 2022, accessed: 25/10/2023. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/3522782

[11] A. Khormali, J. Park, H. Alasmary, A. Anwar, M. Saad, and D. Mohaisen, "Domain name system security and privacy: A contemporary survey," *ScienceDirect*, 2023, accessed: 13/10/2023. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1389128620313001

[12] "Home - dns abuse institute," *DNS Abuse Institute*, 2023, accessed: 13/10/2023. [Online]. Available: https://dnsabuseinstitute.org/

[13] S. Tajalizadehkhoob and R. Weinstein, "Icann reports dns abuse is trending downward globally," *ICANN*, 2022, accessed: 13/10/2023. [Online]. Available: https://www.icann.org/resources/press-material/release-2022-05-17-en

[14] "September 2022 report - dns abuse institute," *DNS Abuse Institute*, 2022, accessed: 13/10/2023. [Online]. Available: https://dnsabuseinstitute.org/wp-content/uploads/2022/09/DNSAI-Intelligence-Report-September-2022-FINAL.pdf

[15] dotmagazine, "Dns abuse: Everyone's problem - building trustworthiness," https://www.dotmagazine.online/issues/the-heart-of-it/building-trustworthiness/dns-abuse, 2022, accessed: 25/10/2023.

[16] WebinarCare, "Dns security statistics 2023 - everything you need to know," https://webinarcare.com/best-dns-security-software/dns-security-statistics/, 2023, accessed: 25/10/2023.

[17] M. Jakobsson and S. Myers, *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. John Wiley & Sons, 2006.

[18] International Trademark Association (INTA), "Inta board resolution on domain name system abuse may 2023," https://www.inta.org/wp-content/uploads/public-files/advocacy/board-resolutions/INTA-Board-Resolution-on-Domain-Name-System-Abuse-May-2023.pdf, 2023, accessed: 25/10/2023.

[19] B. Edelman, "Typosquatting: Unintended adventures in browsing," *McAfee Security Journal*, pp. 34–7, 2008, accessed: 25/10/2023.

[20] D. H. B. C. F. CITP, A. L. CISSP, and C. B. CISSP, "Is your pc a zombie? here's how to avoid the attentions of blacklisters and vampire slayers." accessed: 25/10/2023.

[21] H.-T. Lin, Y.-Y. Lin, and J.-W. Chiang, "Genetic-based real-time fast-flux service networks detection," *Computer Networks*, vol. 57, no. 2, pp. 501–513, 2013, accessed: 25/10/2023.

[22] M. Antonakakis, R. Perdisci, Y. Nadji, N. Vasiloglou, S. Abu-Nimeh, W. Lee, and D. Dagon, "From {Throw-Away} traffic to bots: Detecting the rise of {DGA-Based} malware," in *21st USENIX Security Symposium (USENIX Security 12)*, 2012, pp. 491–506.

[23] J. Frieß, T. Gattermayer, N. Gelernter, H. Schulmann, and M. Waidner, "Cloudy with a chance of cyberattacks: Dangling resources abuse on cloud platforms," in *Proceedings of the 2024 USENIX Conference on Networked Systems Design and Implementation (NSDI'24)*. USENIX Association, 2024, accessed:04/04/2024.

[24] GoDaddy, "Demystifying dns abuse | the godaddy blog," https://www.godaddy.com/resources/skills/demystifying-dns-abuse-understanding-the-digital-threat-landscape, 2023, accessed: 25/10/2023.

[25] R. Böhme, *The economics of information security and privacy*. Springer, 2013, accessed: 25/10/2023.

[26] K. Fowler, *Data breach preparation and response: breaches are certain, impact is not*. Syngress, 2016, accessed: 25/10/2023.

[27] J. Saxe and H. Sanders, *Malware data science: attack detection and attribution*. No Starch Press, 2018, accessed:11/11/2023.

[28] ICANN, "The last four years in retrospect: A brief review of dns abuse trends," https://www.icann.org/en/system/files/files/last-four-years-retrospect-brief-review-dns-abuse-trends-22mar22-en.pdf, 2022, accessed: 25/10/2023.

[29] T. Wrightson, *Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization*, illustrated ed. McGraw-Hill Education, 2014, accessed:11/11/2023.

[30] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (iot) security: Current status, challenges and prospective measures," in *2015 10th international conference for internet technology and secured transactions (ICITST)*. IEEE, 2015, pp. 336–341, accessed:11/11/2023.

[31] M. Dooley and T. Rooney, *DNS Security Management*. John Wiley & Sons, 2017, accessed:11/11/2023.

[32] N. Schick, *Deep fakes and the infocalypse: What you urgently need to know*. Hachette UK, 2020, accessed:11/11/2023.

[33] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud security and privacy: an enterprise perspective on risks and compliance*. " O'Reilly Media, Inc.", 2009, accessed:11/11/2023.

[34] M. H. Au and R. Choo, *Mobile security and privacy: Advances, challenges and future research directions*. Syngress, 2016, accessed:11/11/2023.

[35] I. Bashir and N. Prusty, *Advanced Blockchain Development: Build highly secure, decentralized applications and conduct secure transactions*. Packt Publishing Ltd, 2019, accessed:11/11/2023.

[36] M. Chapple and D. Seidl, *Cyberwarfare: Information operations in a connected world*. Jones & Bartlett Learning, 2021, accessed:11/11/2023.

[37] T. Brunner, "Cybersecurity in beyond 5g: use cases, current approaches, trends, and challenges," *Communication Systems XIV*, p. 28, 2021, accessed:20/11/2023.

[38] S. Boyson, "Cyber supply chain risk management: Revolutionizing the strategic control of critical it systems," *Technovation*, vol. 34, no. 7, pp. 342–353, 2014, accessed:20/11/2023.

[39] ICANN, "Dnssec – what is it and why is it important?" https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en, accessed: 25/10/2023.

[40] M. W. Lucas, *TLS Mastery: Beastie Edition*. Tilted Windmill Press, 2021, accessed:20/11/2023.

[41] S. G. Moghaddam, A. Nasiri, and M. Sharifi, "Ecco mnemonic authentication–two-factor authentication method with ease-of-use," *International Journal of Computer Network and Information Security*, vol. 6, no. 7, p. 11, 2014, accessed:20/11/2023.

[42] F. Skopik, *Collaborative cyber threat intelligence: detecting and responding to advanced cyber attacks at the national level*. CRC Press, 2017, accessed:20/11/2023.

[43] A. S. Coronado, "It auditing: Using controls to protect information assets , by chris davis, mike schiller, and kevin wheeler," 2014, accessed:20/11/2023.

[44] E. Tsukerman, *Machine Learning for Cybersecurity Cookbook: Over 80 recipes on how to implement machine learning algorithms for building security systems using Python*. Packt Publishing Ltd, 2019, accessed:20/11/2023.

[45] J. Meese, "Edited by ramon lobato," 2016, accessed:20/11/2023.

[46] G. Schmid, "Thirty years of dns insecurity: Current issues and perspectives," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2429–2459, 2021, accessed:10/12/2023.

[47] Cloudflare, "Transparency Report H2 2022," 2022, accessed:10/03/2024. [Online]. Available: https://www.cloudflare.com/transparency-reports/transparency-report-h2-2022

[48] Google, "Government removals transparency report," https://transparencyreport.google.com/government-removals/overview?hl=en, 2023, accessed:22/03/2024.

[49] Amazon, "Title of the specific help page," https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF, 2023, accessed:22/03/2024.

[50] Facebook, "Intellectual property transparency report," https://transparency.fb.com/reports/intellectual-property/, 2023, accessed:22/03/2024.

[51] T-Mobile, "2022 transparency report," https://www.t-mobile.com/news/_admin/uploads/2023/07/2022-Transparency-Report.pdf, July 2023, accessed:25/03/2024.

[52] IBM Corporation, "Ibm transparency report," https://www.ibm.com/downloads/cas/DAGAKDJG, 2023, accessed:25/03/2024.

[53] Xiaomi, "Xiaomi transparency report," https://trust.mi.com/transparency, 2023, accessed:25/03/2024.

[54] eBay Inc., "ebay 2022 global transparency report," https://static.ebayinc.com/assets/Uploads/Documents/eBay-2022-Global-Transparency-Report.pdf, 2022, accessed:25/03/2024.

[55] Apple Inc., "Apple transparency report - great britain," https://www.apple.com/legal/transparency/gb.html, 2023, accessed:25/03/2024.

[56] S. Rizvi, M. Scanlon, J. Mcgibney, and J. Sheppard, "Application of artificial intelligence to network forensics: Survey, challenges and future directions," *IEEE Access*, vol. 10, pp. 110 362–110 384, 2022, accessed:10/12/2023.

[57] "Dns security threat mitigation program," ICANN, accessed:02/03/2024. [Online]. Available: https://www.icann.org/dns-security-threat

[58] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, p. 101804, 2023, accessed:05/12/2023.

[59] Messaging Malware and Mobile Anti-Abuse Working Group, "M3AAWG DNS Abuse Prevention Remediation and Mitigation Practices for Registrars and Registries," January 2024, accessed:20/01/2024. [Online]. Available: http://www.m3aawg.org/DNSAbusePreventionRegReg2024

[60] M. Hussain, N. Shah, R. Amin, S. S. Alshamrani, A. Alotaibi, and S. M. Raza, "Software-defined networking: Categories, analysis, and future directions," *Sensors*, vol. 22, no. 15, p. 5551, 2022, accessed:05/12/2023.

[61] T. Goethals, B. Volckaert, and F. De Turck, "Enabling and leveraging ai in the intelligent edge: A review of current trends and future directions," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2311–2341, 2021, accessed:05/12/2023.

[62] dotmagazine.online. (2023) Machine learning and ai in the dns abuse space. Accessed:10/12/2023. [Online]. Available: https://www.dotmagazine.online/issues/building-trust-mitigating-abuse/domain-name-system-topdns-best-practice-webinars/machine-learning-and-ai-in-the-dns-abuse-space

[63] M. B. Halvorsen. (2023) 5 questions for michael b. halvorsen: Machine learning and ai in the dns abuse space. Accessed:10/12/2023. [Online]. Available: https://iq.global/news/5-questions-for-michael-b-halvorsen-machine-learning-and-ai-in-the-dns-abuse-space

[64] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review," *Sensors*, vol. 23, no. 8, p. 4117, 2023, accessed:10/12/2023.

[65] J. Li, "Malicious domain detection based on dns query using machine learning," *ResearchGate*, 2020, accessed:20/12/2023. [Online]. Available: https://www.researchgate.net/publication/333571759_Malicious_domain_detection_based_on_DNS_query_using_Machine_Learning

[66] F. Zou, S. Zhang, W. Rao, and P. Yi, "Detecting malware based on dns graph mining," *ResearchGate*, 2015, accessed:20/12/2023. [Online]. Available: https://www.researchgate.net/publication/282848727_Detecting_Malware_Based_on_DNS_Graph_Mining

[67] M. Antonakakis, R. Perdisci, W. Lee, and D. Dagon, "Detecting malware domains at the upper dns hierarchy," in *ResearchGate*, 2011, accessed:20/12/2023. [Online]. Available: https://www.researchgate.net/publication/220430633_Detecting_malware_domains_at_the_upper_DNS_hierarchy

[68] W. Kumari, G. Aaron, B. Addis, L. Chapin, J. Levine, M. Seiden *et al.*, "Sac115-ssac

report on an interoperable approach to addressing abuse handling in the dns," 2021, accessed:05/12/2023.

[69] P. A. Networks, "Dns attacks in the real world," May 2021, accessed:20/12/2023. [Online]. Available: https://www.paloaltonetworks.com/blog/2021/05/netsec-dns-attacks/

[70] Unit 42, Palo Alto Networks, "xhunt campaign: New backdoors," https://unit42.paloaltonetworks.com/xhunt-campaign-backdoors/, 2021, accessed: 05/01/2024.

[71] ——, "Oilrig uses novel c2 channel and payloads with steganography," https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/, 2021, accessed: 05/01/2024.

[72] ——, "Fireeye, solarstorm and sunburst," https://unit42.paloaltonetworks.com/fireeye-solarstorm-sunburst/, 2021, accessed: 10/01/2024.

[73] ——, "Fast flux 101," https://unit42.paloaltonetworks.com/fast-flux-101/, 2021, accessed: 10/01/2024.

[74] ——, "Covid-19 themed phishing attacks," https://unit42.paloaltonetworks.com/covid-19-themed-phishing-attacks/, 2021, accessed: 10/01/2024.

[75] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Cybersecurity threats, countermeasures and mitigation techniques on the iot: future research directions," *Electronics*, vol. 11, no. 20, p. 3330, 2022, accessed:20/11/2023.

[76] P. V. Roste, "Icann77: Dns abuse measuring, mitigation and the way forward," https://www.centr.org/news/blog/icann77-dns-abuse.html, June 2023, accessed:28/03/2024.

[77] Information Services Group (ISG), "Enterprise security leaders see ai and machine learning as the biggest near-term cyberthreats, isg study finds," *Business Wire*, Aug 2023, accessed:28/03/2024. [Online]. Available: https://www.businesswire.com/news/home/20230815507330/en/Enterprise-Security-Leaders-See-AI-and-Machine-Learning-as-the-Biggest-Near-Term-Cyberthreats-IS

[78] D. Li, "The analysis of conflict and law adjustment between domain name and trademark," *Journal of Dalian Maritime University*, 2002, accessed:20/01/2024. [Online]. Available: https://consensus.app/papers/analysis-conflict-adjustment-domain-name-trademark-dong/9a55a7a1ec665cd0a1c38b36c3e7a67d/

[79] M. Mehta. (2021) 10 interesting cybersquatting examples to learn from. Accessed:20/01/2024. [Online]. Available: https://sectigostore.com/blog/cybersquatting-examples/

[80] P. Security. (2021) 11 types of phishing + real-life examples. Accessed:02/03/2024. [Online]. Available: https://www.pandasecurity.com/en/mediacenter/types-of-phishing/

[81] S. Yu-rong, "On the conflict and legal settlement between domain names and trademarks," *Journal of Beijing University of Technology*, 2006, accessed:04/02/2024. [Online]. Available: https://consensus.app/papers/conflict-legal-settlement-between-domain-names-yurong/c43e797751ae547c8788d5631cca3214/

[82] S. Singh, "Conflicts between trademarks and domain names: A critical analysis," *Intellectual Property: Trademark Law eJournal*, 2011, accessed:04/02/2024. [Online]. Available: https://consensus.app/papers/conflicts-trademarks-domain-names-critical-analysis-singh/cf42588db6be52f6b836f49c9d84404d/

[83] T. Holgers, D. E. Watson, and S. D. Gribble, "Cutting through the confusion: A measurement study of homograph attacks," in *Proceedings of the 2006 USENIX Security Symposium*. Seattle, WA: USENIX Association, July 2006, accessed:02/03/2024.

[84] Cloudflare, Inc. (2023) Cloudflare uses the power of its global network to identify the top 50 most impersonated brands and protect zero trust customers from phishing scams. Accessed:04/02/2024. [Online]. Available: https://www.cloudflare.com/es-es/press-releases/2023/top-50-impersonated-brands-phishing/

[85] "Internationalized domain names (idn) in chromium," accessed:04/02/2024. [Online]. Available: https://chromium.googlesource.com/chromium/src/+/main/docs/idn.md

[86] World Trademark Review, "Domain name registration strategies: new perspectives on an old practice," 2020, accessed:29/02/2024. [Online]. Available: https://www.worldtrademarkreview.com/global-guide/anti-counterfeiting-and-online-brand-enforcement/2020-obe/article/domain-name-registration-strategies-new-perspectives-old-practice

[87] ICANN, "Trademark clearinghouse (tmch)," 2023, accessed:29/02/2024. [Online]. Available: https://newgtlds.icann.org/en/about/trademark-clearinghouse

[88] Trademark Clearinghouse, "What is the trademark clearinghouse?" 2023,

accessed:29/02/2024. [Online]. Available:
https://www.trademark-clearinghouse.com/content/what-trademark-clearinghouse

[89] SOCRadar Cyber Intelligence Inc., "Don't be blinded by what you see: Demystifying homograph attacks," 2023, accessed:15/02/2024. [Online]. Available: https://socradar.io/dont-be-blinded-by-what-you-see-demystifying-homograph-attacks/

[90] Malwarebytes, "Out of character: Homograph attacks explained," 2017, accessed:15/02/2024. [Online]. Available: https://www.malwarebytes.com/blog/news/2017/10/out-of-character-homograph-attacks-explained

[91] Cyber Threat Alliance, "Mitigating dns abuse and safeguarding the internet," 2023, accessed:15/02/2024. [Online]. Available: https://www.cyberthreatalliance.org/value-collaborative-threat-intelligence-sharing/

[92] S. Alder, "44,000 patients impacted by phishing attacks on intermed and spectrum healthcare partners," *HIPAA Journal*, January 2020, accessed:10/03/2024. [Online]. Available: https://www.hipaajournal.com/44000-patients-impacted-by-phishing-attacks-on-intermed-and-spectrum-healthcare-partners/

[93] U. Author, "Phishing email scam stole $100 million from facebook and google," *CNBC*, March 2019, accessed:10/03/2024. [Online]. Available: https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html

[94] Digital Guardian, "Phishing attack prevention: How to identify & prevent phishing attacks," https://www.digitalguardian.com/blog/phishing-attack-prevention-how-identify-prevent-phishing-attacks, 2022, accessed:10/03/2024.

[95] Center for Democracy and Technology, "Prevention and mitigation of successful phishing attacks," https://cdt.org/insights/prevention-and-mitigation-of-successful-phishing-attacks/, March 2022, accessed:15/03/2024.

[96] Y. E. Suzuki and S. A. Salinas Monroy, "Prevention and mitigation measures against phishing emails: a sequential schema model," *Security Journal*, vol. 35, pp. 1162–1182, 2022, accessed:15/03/2024.

[97] T. Chin Jr., K. Xiong, and C. Hu, "Phishlimiter: A phishing detection and mitigation approach using software-defined networking," *IEEE Access*, vol. 6, 2018, accessed:15/03/2024.

[98] S. Catania. (2022) The debate around defining, preventing and mitigating dns abuse. Accessed:04/02/2024. [Online]. Available:

https://www.dotmagazine.online/issues/protecting-users-and-systems/preventing-fighting-abuse-concern/debate-defining-preventing-mitigating-dns-abuse

[99] R. Weinstein. (2023) Icann's contracted parties approve new obligations to mitigate dns abuse. Accessed:15/02/2024. [Online]. Available: https://www.icann.org/en/blogs/details/icanns-contracted-parties-approve-new-obligations-to-mitigate-dns-abuse-13-12-2023-en

[100] ICANN, "Icann's contracted parties approve new obligations to mitigate dns abuse," 2023, accessed:15/02/2024. [Online]. Available: https://www.icann.org/en/blogs/details/icanns-contracted-parties-approve-new-obligations-to-mitigate-dns-abuse-13-12-2023-en

[101] D. A. Institute, "Introducing netbeacon: Providing registrars with actionable, high-quality abuse reports," 2023, accessed:15/02/2024. [Online]. Available: https://dnsabuseinstitute.org/introducing-netbeacon/

[102] B. Xu and E. Albert, "Media censorship in china," https://www.cfr.org/backgrounder/media-censorship-china, 2017, accessed:02/03/2024.

[103] C. Dinu. (2023) What is dns filtering and why does your business need it? Accessed:15/03/2024. [Online]. Available: https://heimdalsecurity.com/blog/dns-filtering/

[104] (2023) What is dns filtering? | secure dns servers. Accessed:15/03/2024. [Online]. Available: https://www.cloudflare.com/en-gb/learning/access-management/what-is-dns-filtering/

[105] A. Bhattacharya, "Dns security in the digital age: The role of international cooperation," 2023, accessed:05/12/2023.

A1 Appendix

A1.1 Detailed Transparency Report and DNS Abuse Mitigation by Cloudflare

- **Abuse Reports and Actions Taken**

  1. Handling Abuse Reports: Among many other DNS abuses, phising, malware, and copyright infringements are most common at
  2. Termination of Services:
     - Suspended Accounts and Dom: In the last half of 2022, Cloudflare claims to be committed to suspending 206 accounts and 530 domains that have proof to host content for Child Sexual Abuse Material (CSAM).
  3. Uniform Domain Name Dispute Resolution Policy (UDRP) Requests: Approximately 21 UDRP requests were handled in the latter half of 2022, which shows that Cloudflare is quite serious about resolving domain disputes amicably.

- **Law Enforcement and Legal Compliance**

  1. Legal Sufficiency Review: Cloudflare will respond only to requests of this kind that meet a legal requirement or exemplary cases. In the sphere of law enforcement, there are court orders and subpoenas.
  2. International Privacy Laws: The company will not allow a state to demand a data reach if the legatees of this state contradict such an approach to privacy dictated by the outside state to Cloudflare. This policy highlights the adherence of Cloudflare to previous and subsequent points of the legal framework.
  3. Emergency Disclosure Requests: In such cases, the company agrees to some level of disclosure when there is a formal requirement for legal follow-up.
  4. National Security Requests: The company claims that it only served transparently and open agencies and other organisations. That is why it appeals

against national security orders that do not adhere to the purpose of transparent informatics company performance.

5. International Data Requests: Respond to foreign government requests on US legal standard cases or case evaluations.

- **Mitigation of DNS Abuse**

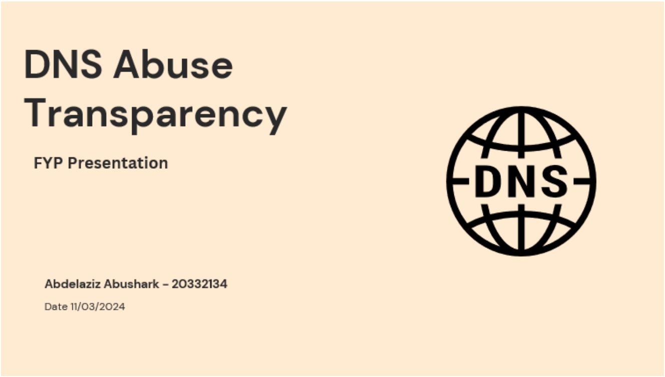
  1. Public Reporting and Transparency: Cloudflare publicly reports and discloses these triggers of abuse, their kinds and quantity, to be able to maintain transparency in the relation of trust that allows ant-abuse to exist.
  2. Law Enforcement Cooperation: Continue your partnerships with law enforcement, ensuring that everything you do is justified from a legal perspective, particularly with respect to DNS abuse.
  3. Challenges to Mitigating DNS Abuse: It is difficult to find a proper balance between the role of each side in defending legal interests and allowing collaborative measures to be accountable for DNS commitment.
  4. Efficiency of efforts: Even with those complications, Cloudflare efficiently mitigates abuse by facilitating root cause solutions and market factor multitude.

- **Proposals for Future Enhancements**

  1. Stakeholder Cooperation: Coordinated law enforcement in service delivery and other roles. Formal collaboration with international organisations and agencies.
  2. Advances in Abuse Detection: The organisation has also developed plans to invest in advanced technologies and machine learning to improve abuse detection and response times.
  3. Transparency Reporting: The organisation has also assured the community of its commitment to further increase the frequency and level of detail in transparency reports this year, describing more clearly the nature and mitigation of DNS abuse.
  4. User Education and Awareness: The organisation has also committed to developing and, more importantly, distributing educational materials aimed at increasing user awareness of the risks related to cybersecurity and DNS abuse.
  5. Policy and Legal Reforms: Because there is likely to be a conflict between privacy laws and external privacy laws, the solution also suggested two law enforcement demands, proposing that participants engage in advocating changes in the resolution of the arising conflict.
  6. Multi-stakeholder Feedback Mechanism: developed and proposed to the Executive Board for adoption and implementation, which outlines feedback

mechanisms that shall include input from users, civil societies, and other stakeholders. This feedback shall form the organisational foundation for improvement and policy formulation.

A1.2 Presentation Slides



DNS Abuse Transparency

FYP Presentation

Abdelaziz Abushark – 20332134

Date 11/03/2024

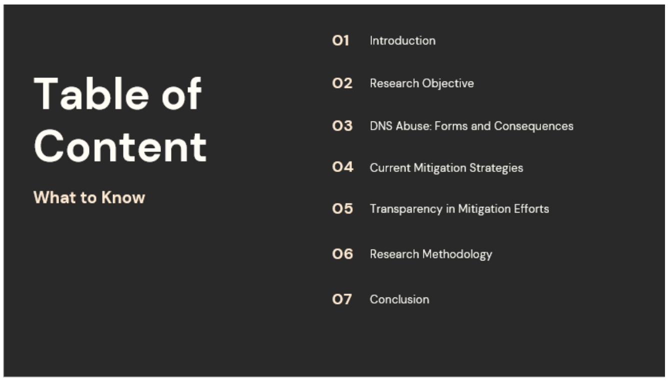


Table of Content

What to Know

01 Introduction

02 Research Objective

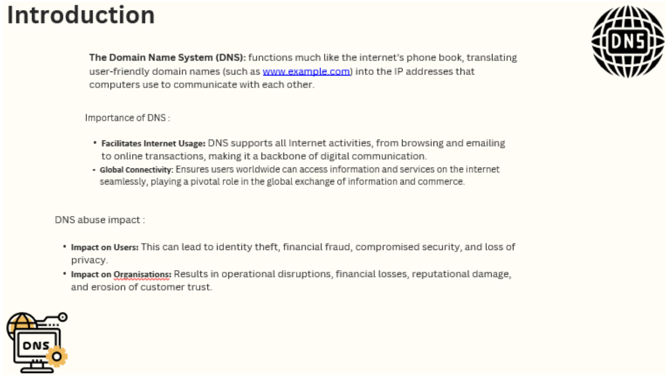
03 DNS Abuse: Forms and Consequences

04 Current Mitigation Strategies

05 Transparency in Mitigation Efforts

06 Research Methodology

07 Conclusion



Introduction

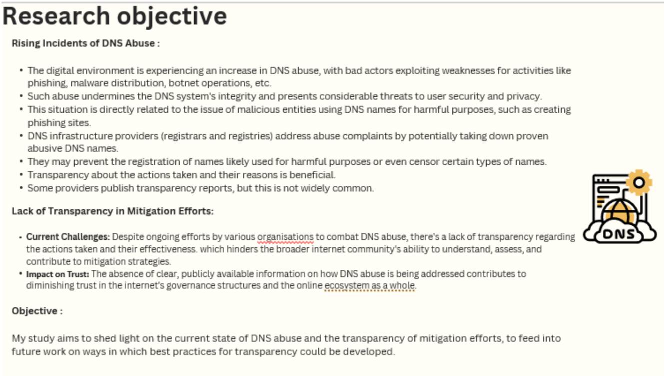
The Domain Name System (DNS): functions much like the internet's phone book, translating user-friendly domain names (such as www.example.com) into the IP addresses that computers use to communicate with each other.

Importance of DNS :

- **Facilitates Internet Usage:** DNS supports all Internet activities, from browsing and emailing to online transactions, making it a backbone of digital communication.
- **Global Connectivity:** Ensures users worldwide can access information and services on the internet seamlessly, playing a pivotal role in the global exchange of information and commerce.

DNS abuse impact :

- **Impact on Users:** This can lead to identity theft, financial fraud, compromised security, and loss of privacy.
- **Impact on Organisations:** Results in operational disruptions, financial losses, reputational damage, and erosion of customer trust.



Research objective

Rising Incidents of DNS Abuse :

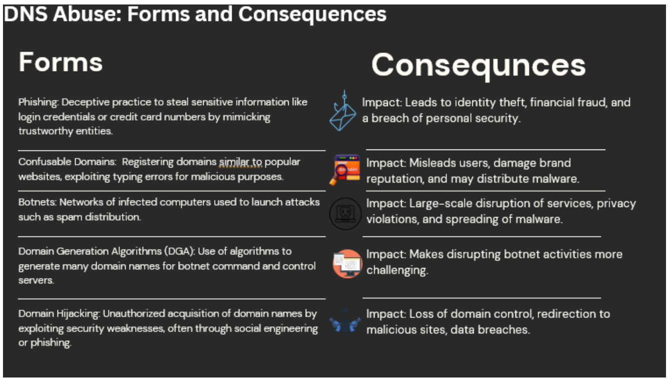
- The digital environment is experiencing an increase in DNS abuse, with bad actors exploiting weaknesses for activities like phishing, malware distribution, botnet operations, etc.
- Such abuse undermines the DNS system's integrity and presents considerable threats to user security and privacy.
- This situation is directly related to the issue of malicious entities using DNS names for harmful purposes, such as creating phishing sites.
- DNS infrastructure providers (registrars and registries) address abuse complaints by potentially taking down proven abusive DNS names.
- They may prevent the registration of names likely used for harmful purposes or even censor certain types of names.
- Transparency about the actions taken and their reasons is beneficial.
- Some providers publish transparency reports, but this is not widely common.

Lack of Transparency in Mitigation Efforts:

- **Current Challenges:** Despite ongoing efforts by various organisations to combat DNS abuse, there's a lack of transparency regarding the actions taken and their effectiveness. which hinders the broader internet community's ability to understand, assess, and contribute to mitigation strategies.
- **Impact on Trust:** The absence of clear, publicly available information on how DNS abuse is being addressed contributes to diminishing trust in the internet's governance structures and the online ecosystem as a whole.

Objective :

My study aims to shed light on the current state of DNS abuse and the transparency of mitigation efforts, to feed into future work on ways in which best practices for transparency could be developed.



DNS Abuse: Forms and Consequences

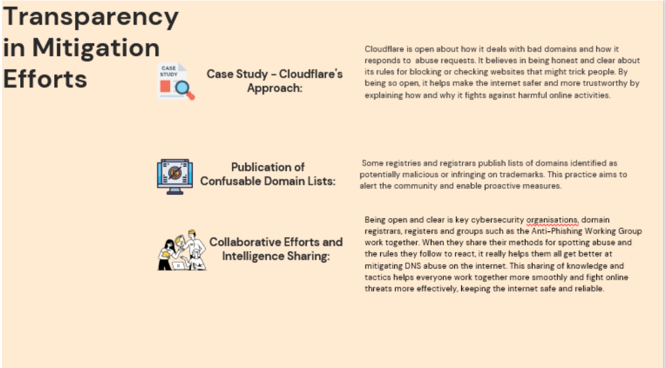
Forms	Consequnces
Phishing: Deceptive practice to steal sensitive information like login credentials or credit card numbers by mimicking trustworthy entities.	Impact: Leads to identity theft, financial fraud, and a breach of personal security.
Confusable Domains: Registering domains similar to popular websites, exploiting typing errors for malicious purposes.	Impact: Misleads users, damage brand reputation, and may distribute malware.
Botnets: Networks of infected computers used to launch attacks such as spam distribution.	Impact: Large-scale disruption of services, privacy violations, and spreading of malware.
Domain Generation Algorithms (DGA): Use of algorithms to generate many domain names for botnet command and control servers.	Impact: Makes disrupting botnet activities more challenging.
Domain Hijacking: Unauthorized acquisition of domain names by exploiting security weaknesses, often through social engineering or phishing.	Impact: Loss of domain control, redirection to malicious sites, data breaches.

Current Mitigation Strategies

Threat Intelligence:

DNS Filtering:

Security Extensions (DNSSEC):



Transparency in Mitigation Efforts

Case Study – Cloudflare's Approach:

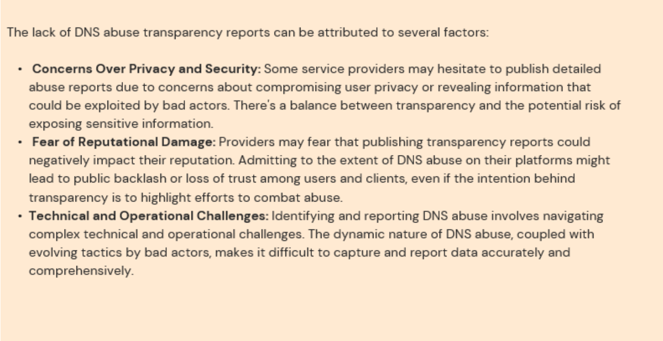
Cloudflare is open about how it deals with bad domains and how it responds to abuse requests. It believes in being honest and clear about its rules for blocking or checking websites that might trick people. By being so open, it helps make the internet safer and more trustworthy by explaining how and why it fights against harmful online activities.

Publication of Confusable Domain Lists:

Some registries and registrars publish lists of domains identified as potentially malicious or infringing on trademarks. This practice aims to alert the community and enable proactive measures.

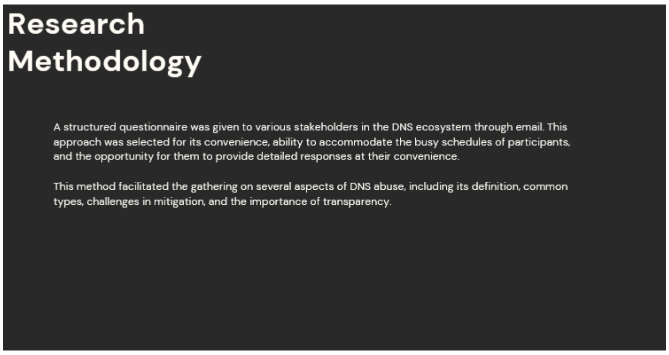
Collaborative Efforts and Intelligence Sharing:

Being open and clear is key cybersecurity organisations, domain registrars, registers and groups such as the Anti-Phishing Working Group work together. When they share their methods for spotting abuse and the rules they follow to react, it really helps them all get better at mitigating DNS abuse on the internet. This sharing of knowledge and tactics helps everyone work together more smoothly and fight online threats more effectively, keeping the internet safe and reliable.



The lack of DNS abuse transparency reports can be attributed to several factors:

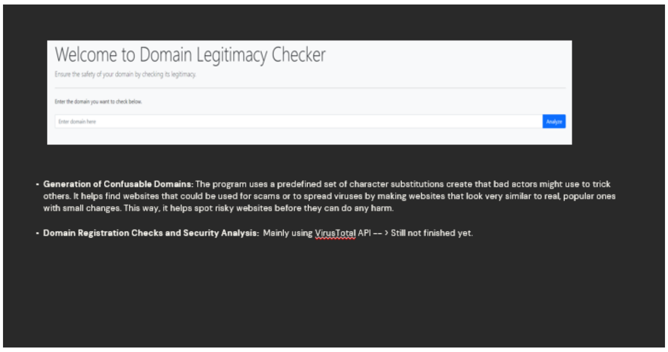
- **Concerns Over Privacy and Security:** Some service providers may hesitate to publish detailed abuse reports due to concerns about compromising user privacy or revealing information that could be exploited by bad actors. There's a balance between transparency and the potential risk of exposing sensitive information.
- **Fear of Reputational Damage:** Providers may fear that publishing transparency reports could negatively impact their reputation. Admitting to the extent of DNS abuse on their platforms might lead to public backlash or loss of trust among users and clients, even if the intention behind transparency is to highlight efforts to combat abuse.
- **Technical and Operational Challenges:** Identifying and reporting DNS abuse involves navigating complex technical and operational challenges. The dynamic nature of DNS abuse, coupled with evolving tactics by bad actors, makes it difficult to capture and report data accurately and comprehensively.



Research Methodology

A structured questionnaire was given to various stakeholders in the DNS ecosystem through email. This approach was selected for its convenience, ability to accommodate the busy schedules of participants, and the opportunity for them to provide detailed responses at their convenience.

This method facilitated the gathering on several aspects of DNS abuse, including its definition, common types, challenges in mitigation, and the importance of transparency.

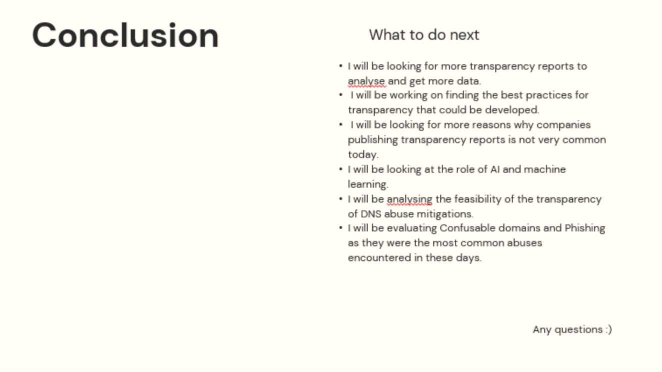


Welcome to Domain Legitimacy Checker

Ensure the safety of your domain by checking its legitimacy.

Enter the domain you want to check below.

- **Generation of Confusable Domains:** The program uses a predefined set of character substitutions create that bad actors might use to trick others. It helps find websites that could be used for scams or to spread viruses by making websites that look very similar to real, popular ones with small changes. This way, it helps spot risky websites before they can do any harm.
- **Domain Registration Checks and Security Analysis:** Mainly using VirusTotal API –– > Still not finished yet.



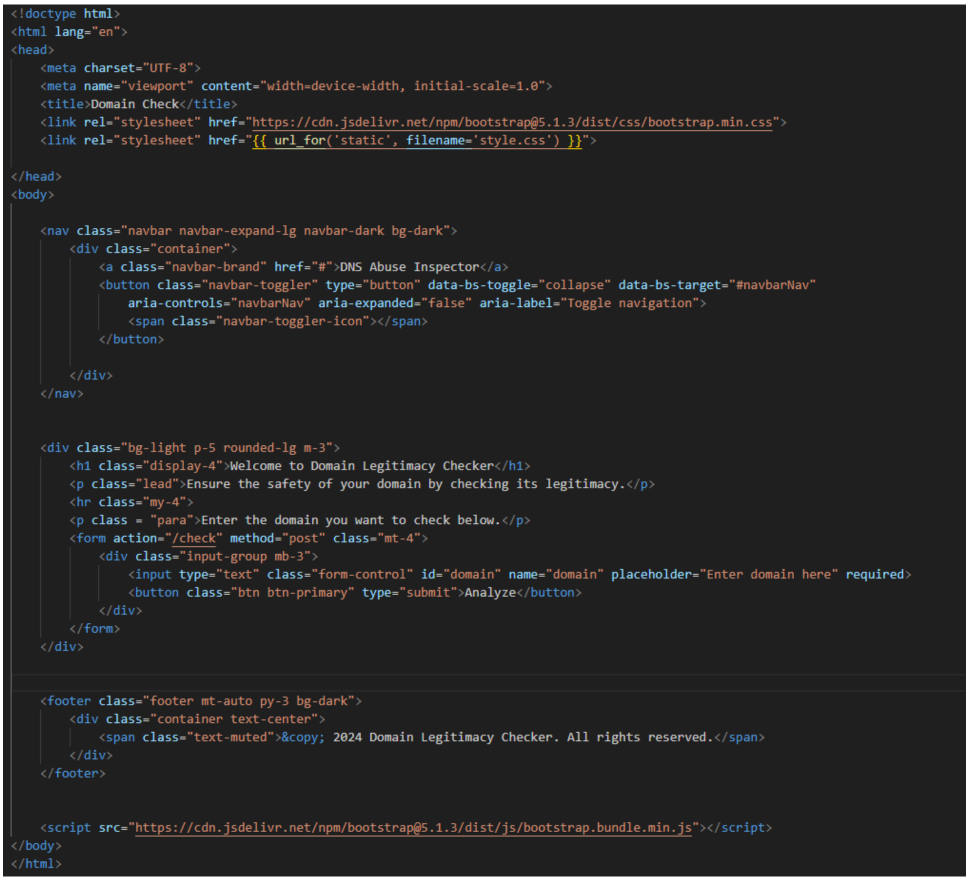
Conclusion

What to do next

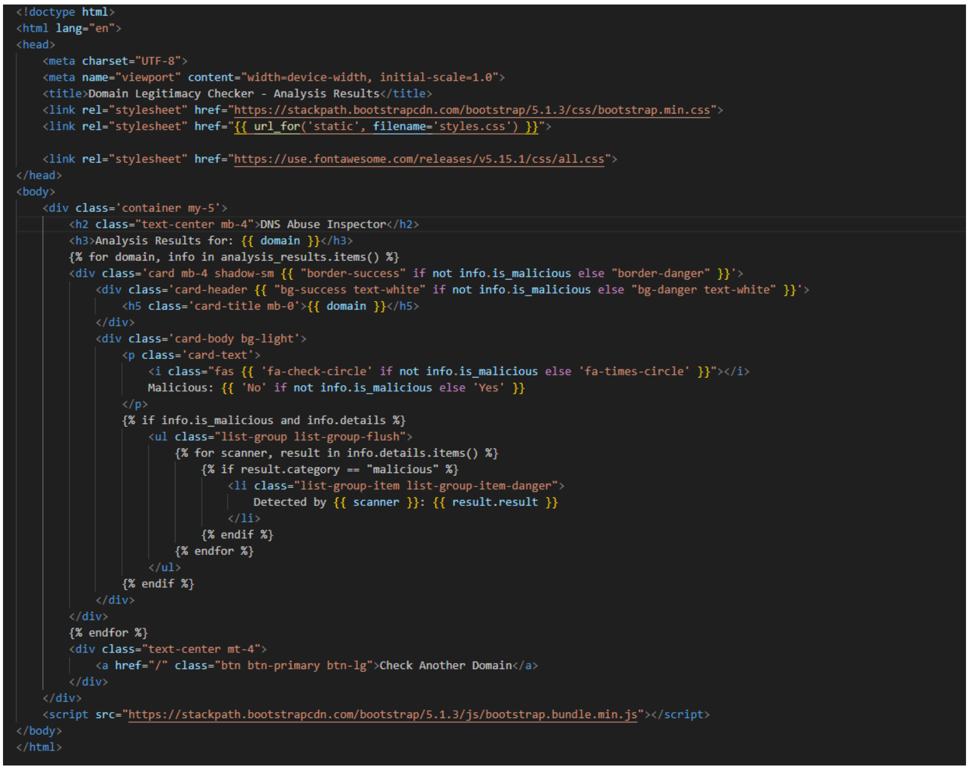
- I will be looking for more transparency reports to analyse and get more data.
- I will be working on finding the best practices for transparency that could be developed.
- I will be looking for more reasons why companies publishing transparency reports is not very common today.
- I will be looking at the role of AI and machine learning.
- I will be analysing the feasibility of the transparency of DNS abuse mitigations.
- I will be evaluating Confusable domains and Phishing as they were the most common abuses encountered in these days.

Any questions :)

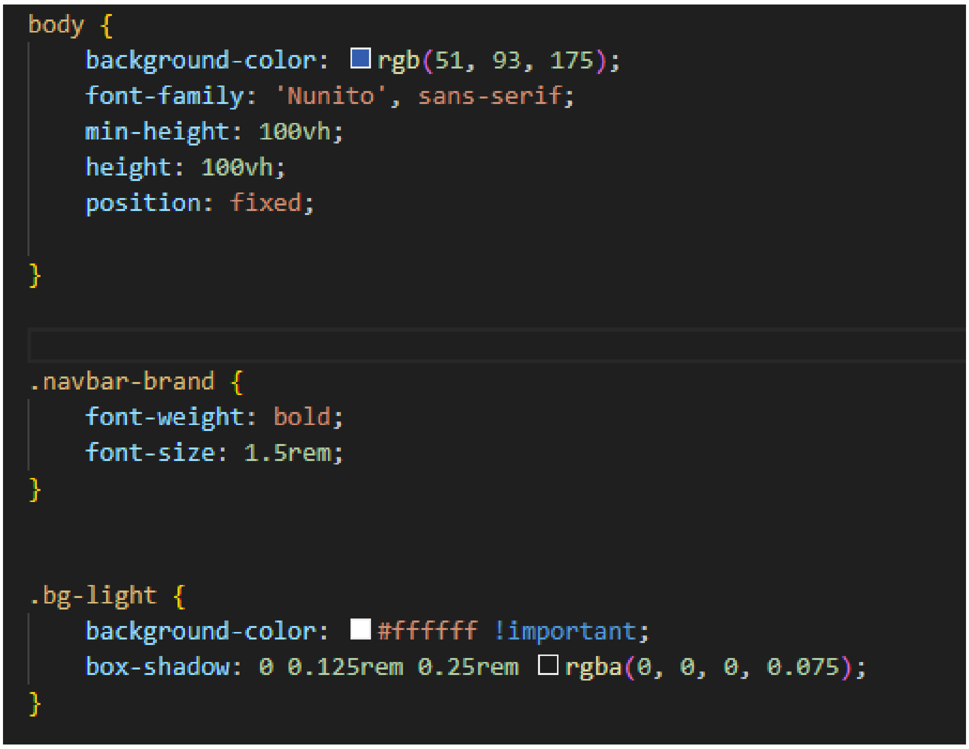
A1.3 Code Screenshots



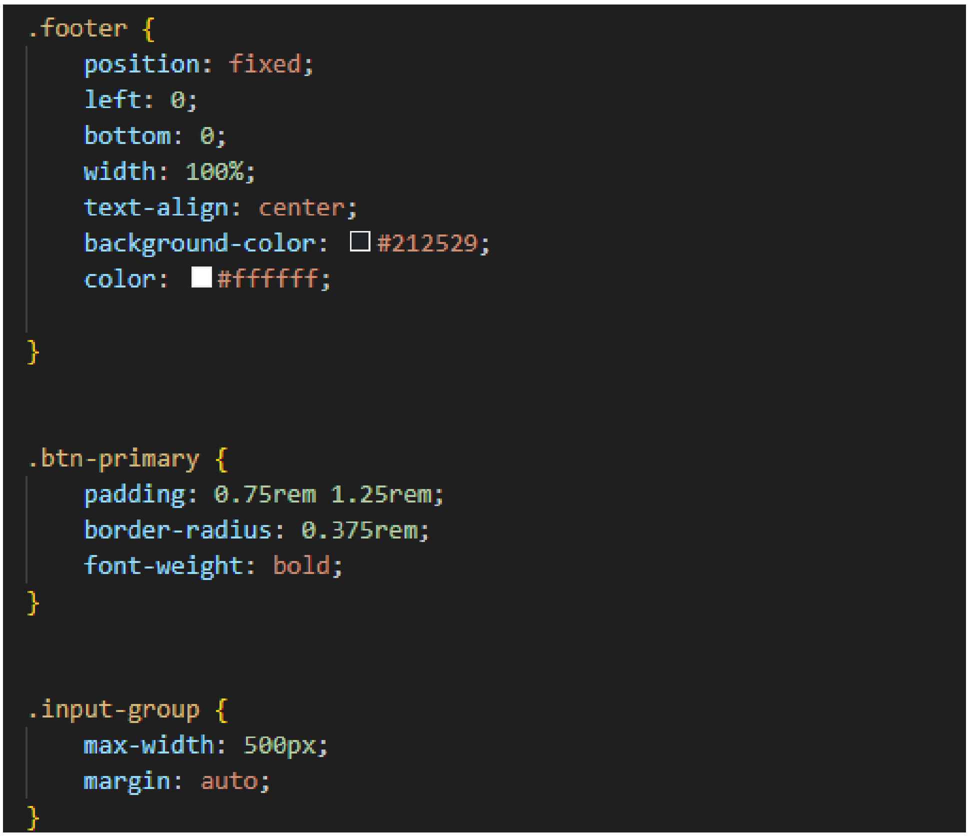
```html
<!doctype html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Domain Check</title>
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/css/bootstrap.min.css">
    <link rel="stylesheet" href="{{ url_for('static', filename='style.css') }}">

</head>
<body>

    <nav class="navbar navbar-expand-lg navbar-dark bg-dark">
        <div class="container">
            <a class="navbar-brand" href="#">DNS Abuse Inspector</a>
            <button class="navbar-toggler" type="button" data-bs-toggle="collapse" data-bs-target="#navbarNav"
                aria-controls="navbarNav" aria-expanded="false" aria-label="Toggle navigation">
                <span class="navbar-toggler-icon"></span>
            </button>

        </div>
    </nav>


    <div class="bg-light p-5 rounded-lg m-3">
        <h1 class="display-4">Welcome to Domain Legitimacy Checker</h1>
        <p class="lead">Ensure the safety of your domain by checking its legitimacy.</p>
        <hr class="my-4">
        <p class = "para">Enter the domain you want to check below.</p>
        <form action="/check" method="post" class="mt-4">
            <div class="input-group mb-3">
                <input type="text" class="form-control" id="domain" name="domain" placeholder="Enter domain here" required>
                <button class="btn btn-primary" type="submit">Analyze</button>
            </div>
        </form>
    </div>


    <footer class="footer mt-auto py-3 bg-dark">
        <div class="container text-center">
            <span class="text-muted">&copy; 2024 Domain Legitimacy Checker. All rights reserved.</span>
        </div>
    </footer>


    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/js/bootstrap.bundle.min.js"></script>
</body>
</html>
```



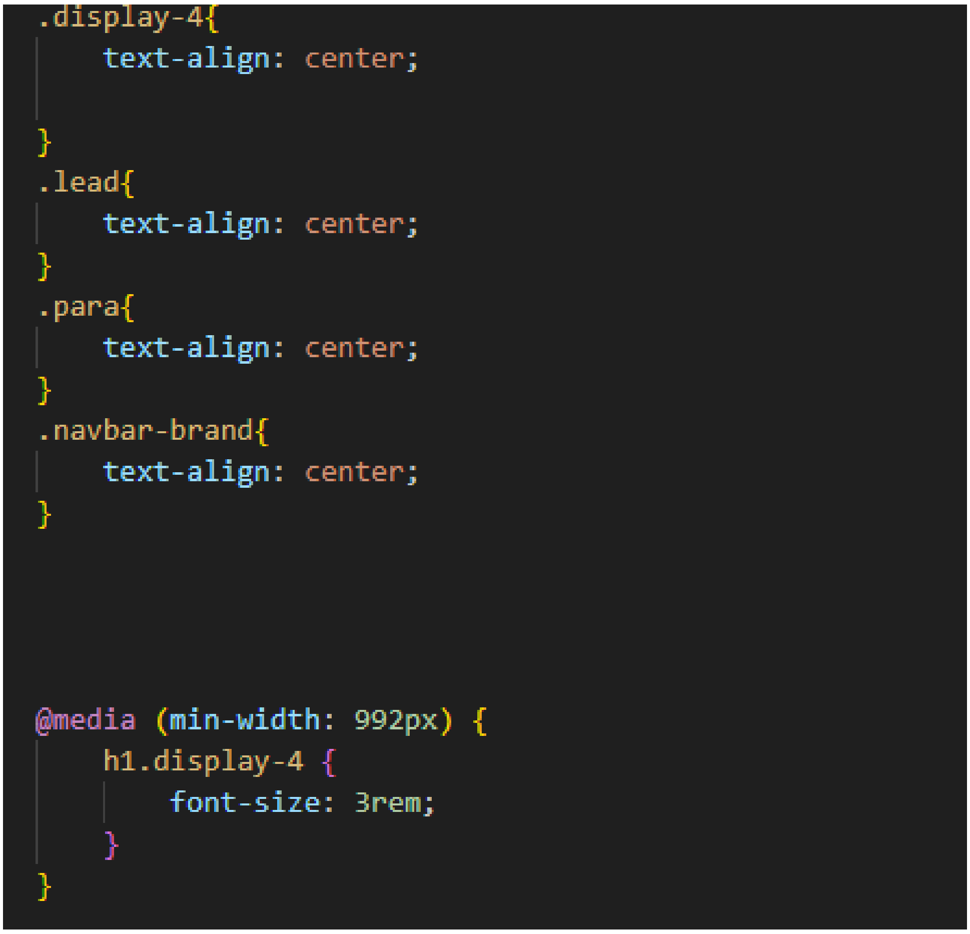
```html
<!doctype html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Domain Legitimacy Checker - Analysis Results</title>
    <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/5.1.3/css/bootstrap.min.css">
    <link rel="stylesheet" href="{{ url_for('static', filename='styles.css') }}">

    <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.15.1/css/all.css">
</head>
<body>
    <div class='container my-5'>
        <h2 class="text-center mb-4">DNS Abuse Inspector</h2>
        <h3>Analysis Results for: {{ domain }}</h3>
        {% for domain, info in analysis_results.items() %}
        <div class='card mb-4 shadow-sm {{ "border-success" if not info.is_malicious else "border-danger" }}'>
            <div class='card-header {{ "bg-success text-white" if not info.is_malicious else "bg-danger text-white" }}'>
                <h5 class='card-title mb-0'>{{ domain }}</h5>
            </div>
            <div class='card-body bg-light'>
                <p class='card-text'>
                    <i class="fas {{ 'fa-check-circle' if not info.is_malicious else 'fa-times-circle' }}"></i>
                    Malicious: {{ 'No' if not info.is_malicious else 'Yes' }}
                </p>
                {% if info.is_malicious and info.details %}
                    <ul class="list-group list-group-flush">
                        {% for scanner, result in info.details.items() %}
                            {% if result.category == "malicious" %}
                                <li class="list-group-item list-group-item-danger">
                                    Detected by {{ scanner }}: {{ result.result }}
                                </li>
                            {% endif %}
                        {% endfor %}
                    </ul>
                {% endif %}
            </div>
        </div>
        {% endfor %}
        <div class="text-center mt-4">
            <a href="/" class="btn btn-primary btn-lg">Check Another Domain</a>
        </div>
    </div>
    <script src="https://stackpath.bootstrapcdn.com/bootstrap/5.1.3/js/bootstrap.bundle.min.js"></script>
</body>
</html>
```



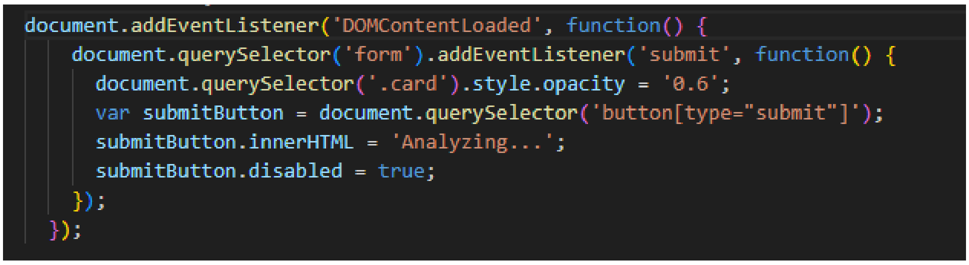
```css
body {
    background-color: rgb(51, 93, 175);
    font-family: 'Nunito', sans-serif;
    min-height: 100vh;
    height: 100vh;
    position: fixed;

}


.navbar-brand {
    font-weight: bold;
    font-size: 1.5rem;
}


.bg-light {
    background-color: #ffffff !important;
    box-shadow: 0 0.125rem 0.25rem rgba(0, 0, 0, 0.075);
}
```



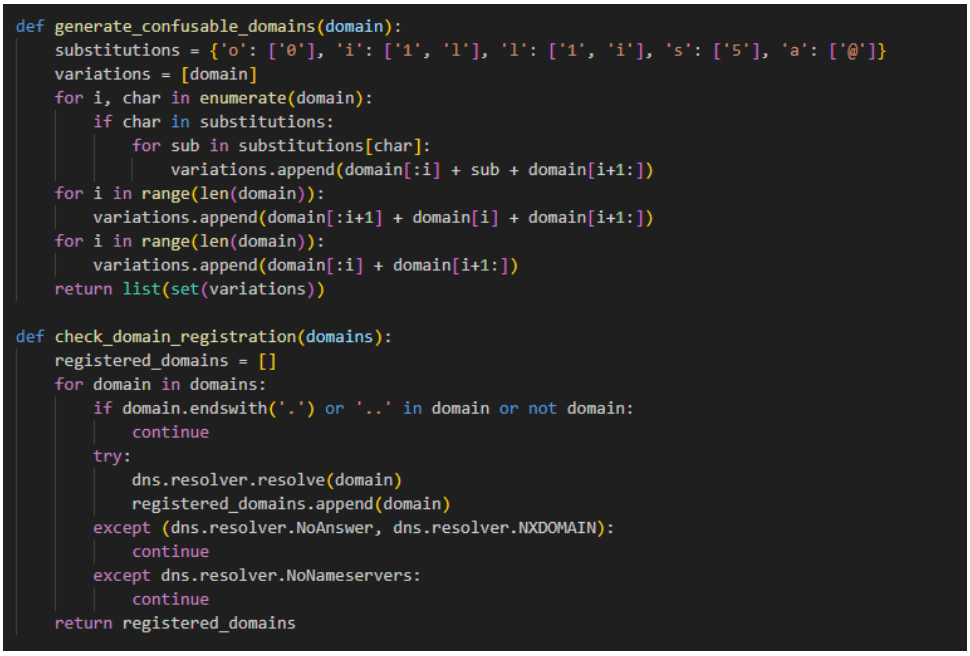
```
.footer {
    position: fixed;
    left: 0;
    bottom: 0;
    width: 100%;
    text-align: center;
    background-color: □#212529;
    color: ■#ffffff;

}


.btn-primary {
    padding: 0.75rem 1.25rem;
    border-radius: 0.375rem;
    font-weight: bold;
}


.input-group {
    max-width: 500px;
    margin: auto;
}
```



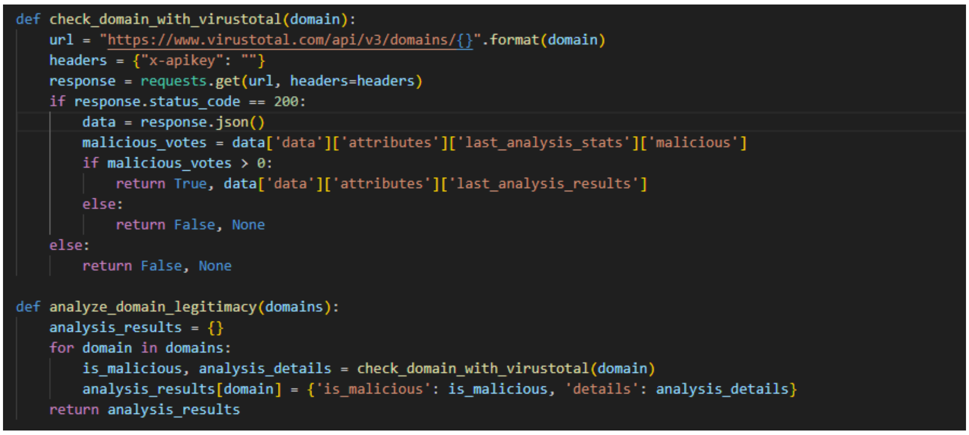
```
.display-4{
    text-align: center;

}
.lead{
    text-align: center;
}
.para{
    text-align: center;
}
.navbar-brand{
    text-align: center;
}




@media (min-width: 992px) {
    h1.display-4 {
        font-size: 3rem;
    }
}
```



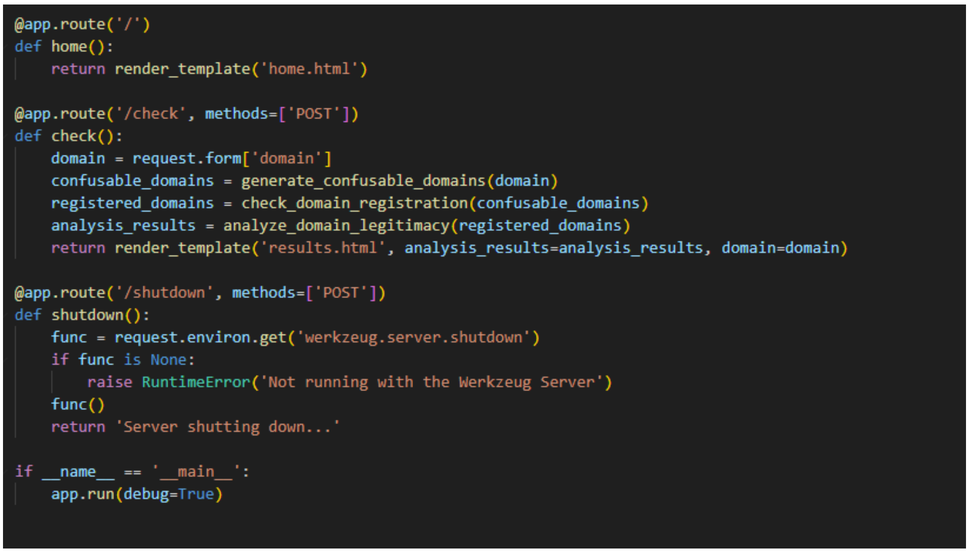
```javascript
document.addEventListener('DOMContentLoaded', function() {
    document.querySelector('form').addEventListener('submit', function() {
      document.querySelector('.card').style.opacity = '0.6';
      var submitButton = document.querySelector('button[type="submit"]');
      submitButton.innerHTML = 'Analyzing...';
      submitButton.disabled = true;
    });
  });
```



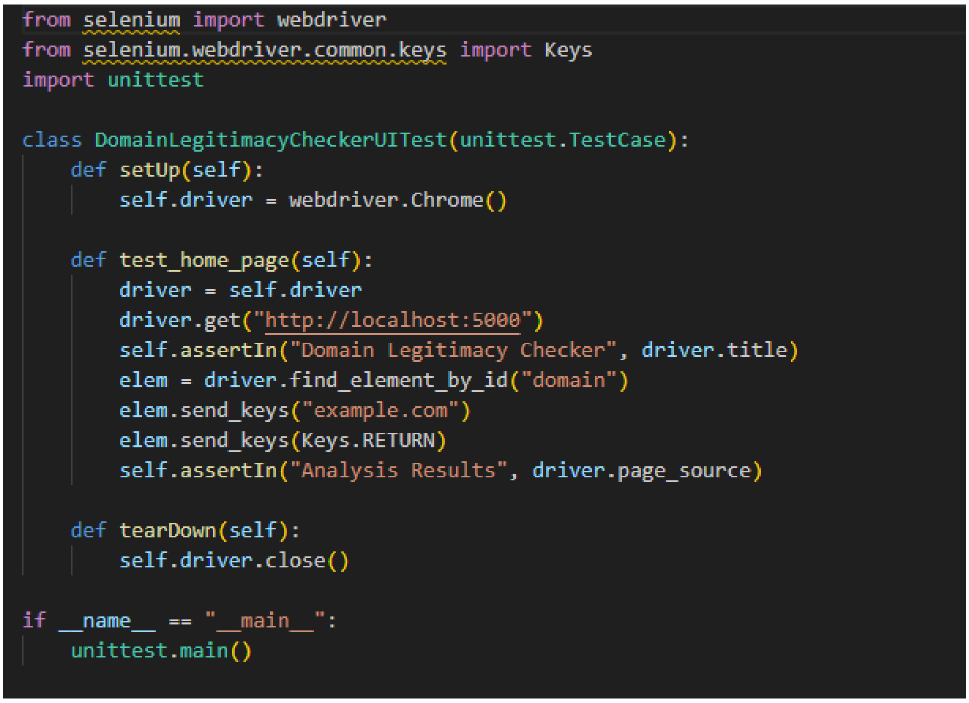
```python
def generate_confusable_domains(domain):
    substitutions = {'o': ['0'], 'i': ['1', 'l'], 'l': ['1', 'i'], 's': ['5'], 'a': ['@']}
    variations = [domain]
    for i, char in enumerate(domain):
        if char in substitutions:
            for sub in substitutions[char]:
                variations.append(domain[:i] + sub + domain[i+1:])
    for i in range(len(domain)):
        variations.append(domain[:i+1] + domain[i] + domain[i+1:])
    for i in range(len(domain)):
        variations.append(domain[:i] + domain[i+1:])
    return list(set(variations))

def check_domain_registration(domains):
    registered_domains = []
    for domain in domains:
        if domain.endswith('.') or '..' in domain or not domain:
            continue
        try:
            dns.resolver.resolve(domain)
            registered_domains.append(domain)
        except (dns.resolver.NoAnswer, dns.resolver.NXDOMAIN):
            continue
        except dns.resolver.NoNameservers:
            continue
    return registered_domains
```



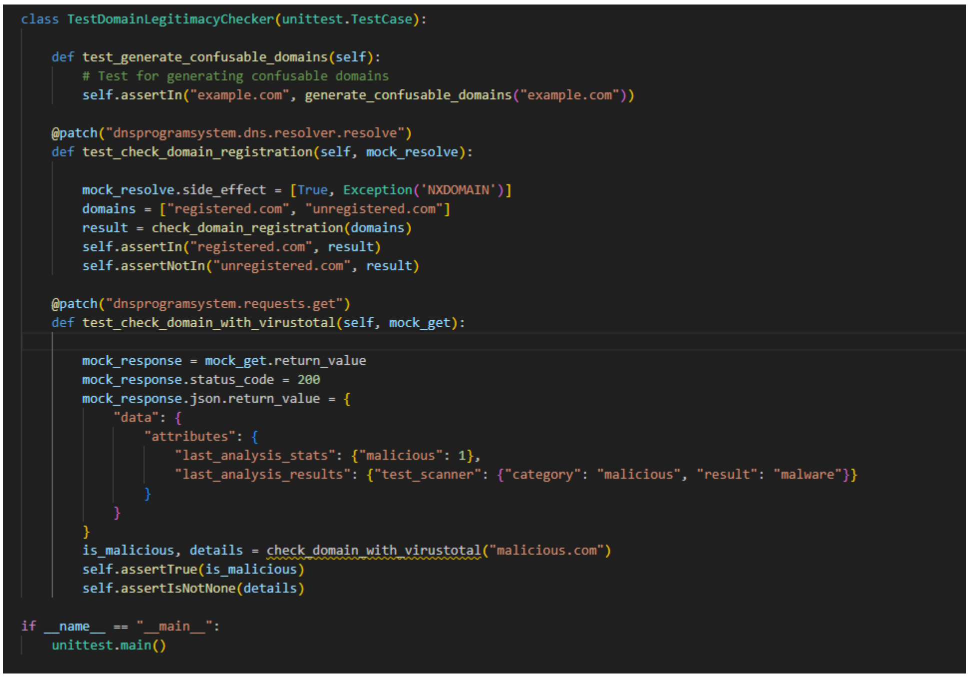
```python
def check_domain_with_virustotal(domain):
    url = "https://www.virustotal.com/api/v3/domains/{}".format(domain)
    headers = {"x-apikey": ""}
    response = requests.get(url, headers=headers)
    if response.status_code == 200:
        data = response.json()
        malicious_votes = data['data']['attributes']['last_analysis_stats']['malicious']
        if malicious_votes > 0:
            return True, data['data']['attributes']['last_analysis_results']
        else:
            return False, None
    else:
        return False, None

def analyze_domain_legitimacy(domains):
    analysis_results = {}
    for domain in domains:
        is_malicious, analysis_details = check_domain_with_virustotal(domain)
        analysis_results[domain] = {'is_malicious': is_malicious, 'details': analysis_details}
    return analysis_results
```



```
@app.route('/')
def home():
    return render_template('home.html')

@app.route('/check', methods=['POST'])
def check():
    domain = request.form['domain']
    confusable_domains = generate_confusable_domains(domain)
    registered_domains = check_domain_registration(confusable_domains)
    analysis_results = analyze_domain_legitimacy(registered_domains)
    return render_template('results.html', analysis_results=analysis_results, domain=domain)

@app.route('/shutdown', methods=['POST'])
def shutdown():
    func = request.environ.get('werkzeug.server.shutdown')
    if func is None:
        raise RuntimeError('Not running with the Werkzeug Server')
    func()
    return 'Server shutting down...'

if __name__ == '__main__':
    app.run(debug=True)
```



```
from selenium import webdriver
from selenium.webdriver.common.keys import Keys
import unittest

class DomainLegitimacyCheckerUITest(unittest.TestCase):
    def setUp(self):
        self.driver = webdriver.Chrome()

    def test_home_page(self):
        driver = self.driver
        driver.get("http://localhost:5000")
        self.assertIn("Domain Legitimacy Checker", driver.title)
        elem = driver.find_element_by_id("domain")
        elem.send_keys("example.com")
        elem.send_keys(Keys.RETURN)
        self.assertIn("Analysis Results", driver.page_source)

    def tearDown(self):
        self.driver.close()

if __name__ == "__main__":
    unittest.main()
```



```python
class TestDomainLegitimacyChecker(unittest.TestCase):

    def test_generate_confusable_domains(self):
        # Test for generating confusable domains
        self.assertIn("example.com", generate_confusable_domains("example.com"))

    @patch("dnsprogramsystem.dns.resolver.resolve")
    def test_check_domain_registration(self, mock_resolve):

        mock_resolve.side_effect = [True, Exception('NXDOMAIN')]
        domains = ["registered.com", "unregistered.com"]
        result = check_domain_registration(domains)
        self.assertIn("registered.com", result)
        self.assertNotIn("unregistered.com", result)

    @patch("dnsprogramsystem.requests.get")
    def test_check_domain_with_virustotal(self, mock_get):

        mock_response = mock_get.return_value
        mock_response.status_code = 200
        mock_response.json.return_value = {
            "data": {
                "attributes": {
                    "last_analysis_stats": {"malicious": 1},
                    "last_analysis_results": {"test_scanner": {"category": "malicious", "result": "malware"}}
                }
            }
        }
        is_malicious, details = check_domain_with_virustotal("malicious.com")
        self.assertTrue(is_malicious)
        self.assertIsNotNone(details)

if __name__ == "__main__":
    unittest.main()
```