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: Research Fellow Stephen Farrell

February 25, 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

A short summary of the problem investigated, the approach taken and the key findings. This should not be more that around 400 words.

This must be on a separate page.

Lay Abstract

Similar to the actual abstract in terms of the information, but written for a non-specialist. So no jargon, no acronyms. Explain to a member of the general public what this project entailed. Should be no longer than the actual abstract.

This must be on a separate page.

Acknowledgements

Thanks Everyone!

You should acknowledge any help that you have received (for example from technical staff), or input provided by, for example, a company.

Contents

List of Figures

List of Tables

Nomenclature

A	Area of the wing	m^2
B		
C	Roman letters first, with capitals...	
a	then lower case.	
b		
c		
Γ	Followed by Greek capitals...	
α	then lower case greek symbols.	
β		
ϵ		
TLA	Finally, three letter acronyms and other abbreviations arranged alphabetically	

If a parameter has a typical unit that is used throughout your report, then it should be included here on the right hand side.

If you have a very mathematical report, then you may wish to divide the nomenclature list into functions and variables, and then sub- and super-scripts.

If you have a large number of acronyms, check out to make that more robust.

Note that Roman mathematical symbols are typically in a serif font in italics.

1 Introduction

1.1 Brief Context for the Problem

The Domain Name System (DNS), which turns domain names into IP addresses, is a crucial element in the large and complex network of digital communications. This system has an impact on each user's everyday digital interactions in addition to ensuring the internet runs smoothly. Unfortunately, this important system is not resistant to abuse. Malicious actors use DNS domains for a variety of illegal activities, such as sending malware, phishing websites, and controlling botnets [1]. These actions compromise the reliability and security of the Internet by posing serious risks to cybersecurity and user trust [2].

The abuse of DNS extends beyond mere inconvenience; it is a serious flaw in the Internet's architecture that might have a big impact on people's privacy, business security, and national security. Abuse techniques are numerous and constantly changing; they include typosquatting, which is the practice of creating malicious domains that imitate real ones, and domain hijacking [3]. These strategies can all have disastrous outcomes, ranging from the theft of private information to the shutdown of important internet services.

DNS security and mitigation of DNS abuse are critical due to its central role in internet operations. To counter these dangers, constant monitoring and proactive steps are needed. This includes communication between numerous parties, such as hosting companies, domain registrars, security researchers, and law enforcement, in addition to technology solutions [4].

1.2 Motivation

The Domain Name System (DNS) is a vital element of web activity in the age of technology, but malicious actors are growing more interested in the system. The DNS abuse for illegal activities such as typosquatting and phishing has raised questions about the integrity and security of the Internet. The severity and frequency of these concerns are highlighted in recent studies, such as the "Study on Domain Name System (DNS) Abuse: Technical Report" by Bayer et al. [2], highlighting the importance of more monitoring and mitigation tactics.

Not only have significant cases of DNS abuse endangered the security of users, but they have also damaged the general trust in the digital economy. Users' trust in online services declines as they become more aware of these hazards, necessitating the implementation of mitigation measures to regain confidence and guarantee a secure online experience. According to Hesselman et al. [5], the idea of a "responsible Internet" aims to boost confidence and sovereignty by improving network-level transparency, accountability, and controllability. Furthermore, Mathew and Cheshire's [6] study "Trust and Community in the Practice of Network Security" dives into the significance of trust connections and communities in cybersecurity, demonstrating the negative effects of DNS abuse on user trust.

Organisations are leading the way in this issue, especially DNS infrastructure providers like registrars and registries. Nevertheless, their policies and activities tend not to be sufficiently clear. The continuous lack of confidence is exacerbated by the unclear way in which DNS abuse allegations are handled and the actions that follow. The importance of protecting the Internet and its reliability is recognised in relation to this issue [7]. These difficulties are compounded by the average user's short attention span and diminished ability to comprehend information, as demonstrated by cognitive psychology studies like Medvedskaya's [8] investigation of adult Internet users' attention spans. According to this research, consuming digital media may have a detrimental effect on one's capacity for sustained concentration, which would make grasping complicated topics even more difficult.

Furthermore, there are ethical and legal consequences to DNS abuse and how to mitigate it in addition to the technical ones. The goal of this project is to close this gap by investigating ways to improve the transparency of DNS abuse mitigation. This study aims to shine light on the present efforts and highlight the obstacles to greater transparency by assessing the current landscape of transparency reports and practices among DNS infrastructure providers. The ultimate objective is to provide a contribution to a system that promotes and enables more efficient and approachable transparency in DNS abuse mitigation.

1.3 Research Question/Project and Personal objective

1.3.1 Research Question

The primary research question for this project is: "What strategies and practices are registries, registrars, and other parties involved in DNS infrastructure utilizing to mitigate DNS abuse, and how do the transparency reports available from these entities characterize and reflect their efforts? Furthermore, how could these practices and reports inform the development of best-practices for transparency in handling DNS abuse complaints? This question seeks to uncover the mechanisms, policies, and practices in place to mitigate DNS abuse and to what extent these efforts are transparent to the public and stakeholders.

1.3.2 Project Objectives

Assess Handling of Abuse Complaints :

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

Evaluate Transparency Levels :

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

Benchmark against Best Practices:

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

Develop Recommendations :

- Propose actionable recommendations for DNS infrastructure providers to improve their abuse handling and transparency.
- Suggest policy changes or initiatives that could standardise and improve practices in the industry.

Contribute to Stakeholder Understanding :

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

1.4 Scope

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

1.5 Outline of the Project Work

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

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

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

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

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

1.6 Outline of the report

not finished yet but will include background, state of art, research, implementation, evaluation, discussion, and conclusions.

2 Background

2.1 Introduction

This chapter will explore the fundamental information relevant to this project, with an emphasis on the world of DNS abuse and transparency. It will include a thorough investigation of the domain name system (DNS), its crucial function in the online community, and the variety of abuses it faces. The history of widely used policies and organisations aimed at stopping DNS abuse, including a thorough examination of the DNS Abuse Institute and its achievements, is essential to our investigation. A 'competition landscape' providing a critical examination of current market choices, from automated solutions to human tactics, will be provided as we navigate through the current methodology and technology deployed to mitigate DNS abuse. This analysis will also cover new developments that aim to improve DNS security and privacy, providing information on the use and consequences of technologies such as DNS over TLS (DoT) and DNS over HTTPS (DoH). The reader will obtain an in-depth understanding of the current situation of DNS abuse and the need for a more open, strong, and proactive strategy by analysing these various techniques and appreciating their strengths and weaknesses. This chapter emphasises the importance of the suggested solution in an era where digital authenticity is crucial, 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.

2.2 Understanding DNS and Its Vulnerabilities

The Domain Name System (DNS) is a crucial part of the infrastructure of the Internet, serving as the key that converts computer-understandable IP addresses into human-friendly domain names. Although the DNS plays a vital role in maintaining ongoing online activities, privacy and security problems still arise. The ScienceDirect paper "Domain Name System Security and Privacy: A Contemporary Survey" provides a thorough analysis of these concerns. This survey highlights the fundamental significance of the DNS while illuminating the weaknesses that malicious actors may take advantage of [9].

A variety of security threats exist, ranging from DNS infrastructure-targeting distributed denial of service (DDoS) assaults to cache poisoning and hijacking. Each of these attacks has the potential to do significant harm, including interruptions in service and the promotion of theft and spying. Due to the standard DNS design's lack of encryption, users' query data is vulnerable to abuse and eavesdropping, raising serious privacy problems. However, weaknesses do not mark the end of the story. In the same survey, new approaches are examined to improve DNS security and privacy. The use of DNSSEC (DNS Security Extensions), which authenticates DNS data and guarantees its integrity while repelling some types of attack, is one example of these advances in cryptographic security measures. Moreover, privacy-enhancing technologies are being used to encrypt DNS queries, preventing eavesdropping and manipulation, such as DNS over HTTPS (DoH) and DNS over TLS (DoT).

The environment of DNS threats and defences is always changing in sync with the internet. For systems to be robust and resilient, it is essential to understand these weaknesses and the continuous efforts being made to mitigate them. An in-depth discussion of DNS vulnerability details, the effects of these safety concerns, and creative solutions that aim to bring in a new era of DNS security and privacy will be provided in this section [9].

2.3 Current efforts and organisations combatting DNS Abuse

The DNS Abuse Institute, which will focus on DNS abuse to help in increasing safety and security through the domain name system, is going to be cantered on these efforts to address DNS abuse with a comprehensive approach throughout the infrastructure of the internet. It helps the internet community in the identification, reporting, and mitigation of DNS abuse in its quest to make the online environment more secure. Efforts by the institute, such as Compass Dashboards, provide vital data to registries and registrars that will enable proper decisions on combating misuse. They prove the commitment towards transparency and education by issuing publications like the "DNSAI 2022 Annual Report" or "DNSAI Bulletin 2023 04; Account Takeovers," which provide insights regarding DNS abuse and how they are mitigated. [10] 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 and operability of the Internet. These participatory pillars hint at concerted efforts via policy development, technological developments, and stakeholder engagement as core in this collective approach towards combating DNS abuse [12].

2.4 DNS Privacy and Security Enhancements

The digital world is changing, and so too is the need for enhanced privacy and security measures within the Domain Name System (DNS). Significant advancements have been made to protect users and their data, particularly through the implementation of DNS over TLS (DoT) and DNS over HTTPS (DoH). These technologies represent a paradigm shift in DNS query encryption, aiming to address privacy concerns and secure communication between clients and servers. DNS over TLS (DoT) offers a way to encrypt DNS requests and answers, making it harder for bad actors to simply intercept or change the data. This technology is essential to protect user privacy and stop man-in-the-middle and eavesdropping attacks. In the same way, DNS over HTTPS (DoH) leverages the security features and broad acceptance of HTTPS to protect DNS requests within the HTTPS protocol, adding an extra degree of protection.

The paper "DNS Privacy in Practice and Preparation," which focuses on how these technologies are being accepted and put into effect, provides an in-depth review of these developments. It emphasises how important DoT and DoH are to protecting DNS privacy and how key public DNS service providers are supporting these more and more. The implementation of DoT and DoH is not without difficulties, regardless of their advantages. Their effectiveness depends on factors like performance concerns and the requirement for extensive implementation across multiple platforms. The study also highlights how critical TCP Fast Open (TFO) is to reducing TCP-based DNS query latency, which is essential to balance privacy and speed [11] .

2.5 Different Forms of DNS Abuse

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

2.5.1 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.[17]
- **Mechanism:** This deception often occurs through emails or messaging services that direct users to websites resembling authentic ones.[18]

- **Impact:** Victims may suffer identity theft, financial fraud, and security compromise.

2.5.2 Confusable Domains (Typosquatting)

- **Description:** Registering domain names that look visually similar to popular websites, taking advantage of typing errors or character similarities.[19]
- **Mechanism:** Users may accidentally visit these websites when making a typo in a URL, potentially exposing them to malware or phishing attempts.
- **Impact:** Deception of users and potential harm to brand reputation.[20]

2.5.3 Domain Hijacking

- **Description:** Unauthorized acquisition of domain names by exploiting security vulnerabilities in the domain registration system.[19]
- **Mechanism:** Attackers may use tactics like social engineering, phishing, or exploiting security loopholes to gain control over a domain.
- **Impact:** Loss of website control, redirection to malicious sites, and potential data breaches.

2.5.4 Botnets

- **Description:** Botnets involve controlling a group of computers infected with malware, used to carry out attacks or spread spam and malware.[21]
- **Mechanism:** Malware infects unsuspecting users' computers, incorporating them into a network under the attacker's control.
- **Impact:** Can result in large-scale DDoS attacks, mass spam campaigns, and widespread malware dissemination.

2.5.5 Fast Flux Hosting

- **Description:** A technique used to conceal the location of websites associated with phishing and malware distribution.[22]
- **Mechanism:** Involves a network of compromised hosts that regularly modify DNS records to evade detection.
- **Impact:** Makes tracking and shutting down malicious sites difficult.

2.5.6 Domain Generation Algorithms (DGA)

- **Description:** DGAs generate domain names that act as meeting points for botnets.[23]
- **Mechanism:** Malicious software uses algorithms to generate a sequence of domain names for command-and-control servers.
- **Impact:** Adds complexity to efforts to disrupt botnet command and control channels.

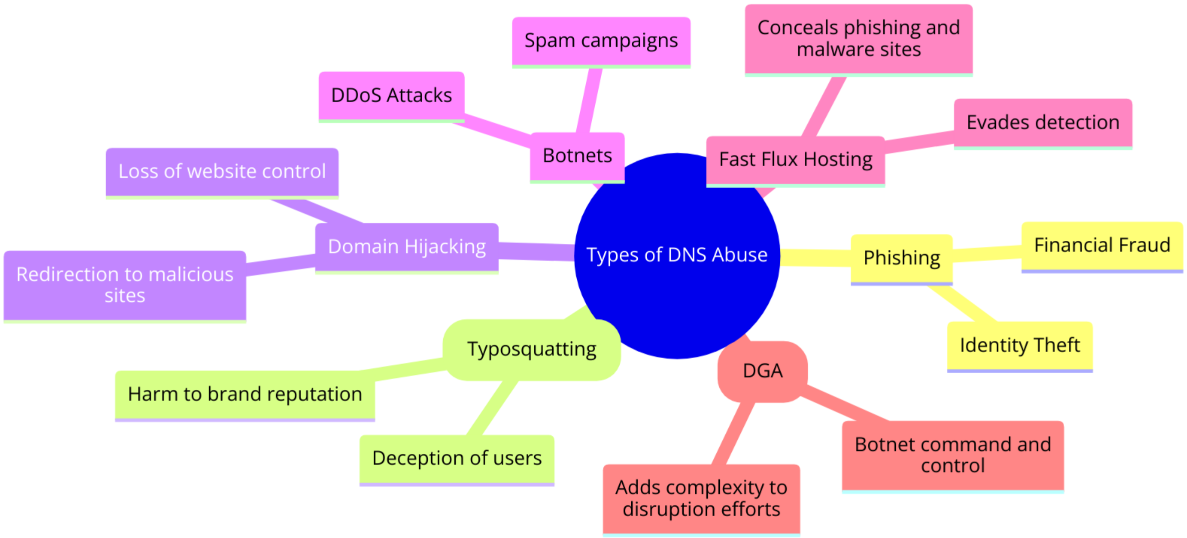

Figure 2.1: Impact of DNS Abuse

2.6 How DNS Abuse Harms Users

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

2.6.1 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.[18, 24]

2.6.2 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.[24, 25]

2.6.3 Data Breach

- **Malware:** Malicious software spread through compromised DNS systems can allow unauthorized access to corporate data, leading to data breaches.[26, 27]

2.6.4 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.[28, 29]

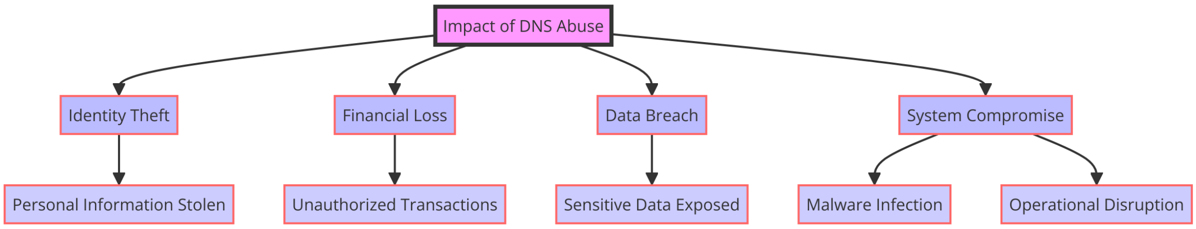

Figure 2.2: Different Forms of DNS Abuse

2.7 Future Dangers of DNS Abuse

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

2.7.1 Increased Sophistication

- **Evolving Techniques:** Cyber attackers are constantly developing more sophisticated techniques to exploit DNS, such as advanced phishing schemes and malware distribution.[26, 30]

2.7.2 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.[31, 32]

2.7.3 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.[28, 33]

2.7.4 Deepfakes and 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.[26, 34]

2.7.5 Cloud Computing Vulnerabilities

- **Targeting Cloud Services:** As organizations increasingly rely on cloud-based services, cybercriminals are exploiting DNS vulnerabilities to attack these platforms, potentially leading to data breaches and service disruptions.[35]

2.7.6 Mobile Device Exploitation

- **Mobile DNS Attacks:** The rising usage of mobile devices has led cybercriminals to target smartphones and tablets through DNS-based attacks, which can lead to data theft and the spread of malware.[36]

2.7.7 Cryptocurrency and 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.[37]

2.7.8 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.[38]

2.7.9 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.[39]

2.7.10 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 organizations.[40]

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.

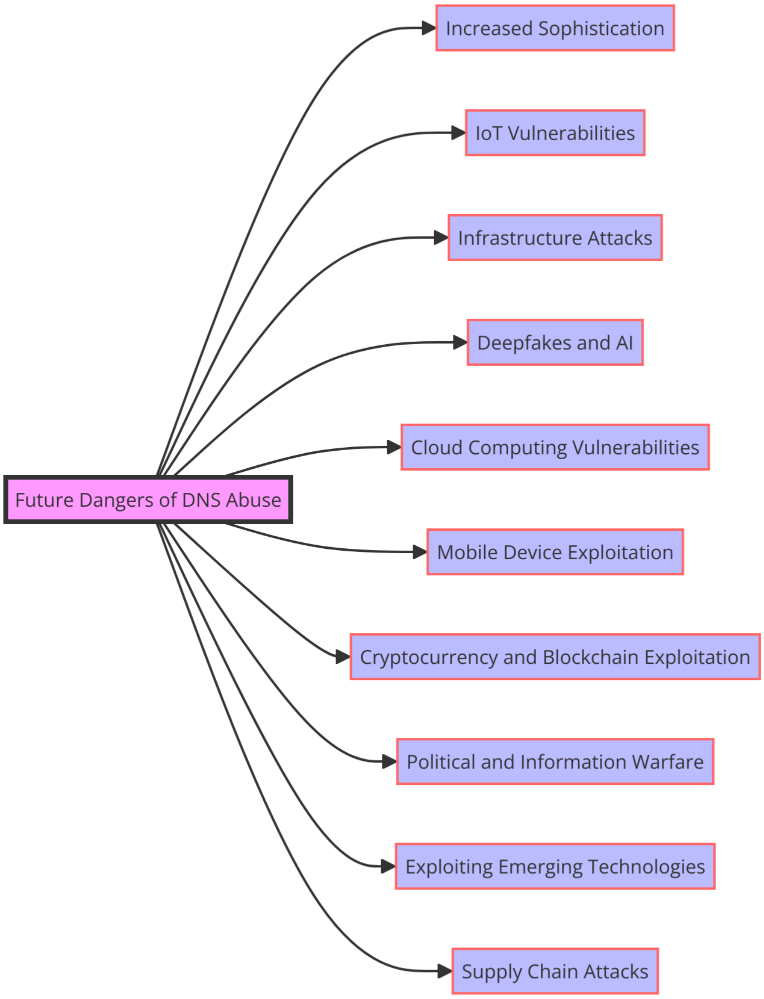
Future Dangers of DNS Abuse
Increased Sophistication
IoT Vulnerabilities
Infrastructure Attacks
Deepfakes and AI
Cloud Computing Vulnerabilities
Mobile Device Exploitation
Cryptocurrency and Blockchain Exploitation
Political and Information Warfare
Exploiting Emerging Technologies
Supply Chain Attacks

Figure 2.3: Future dangers of DNS abuse

2.8 Foundational Mitigation Strategies and Best Practices

To address the broad nature of the threats, combating DNS abuse requires an integrated strategy that integrates multiple strategies and best practices. Setting up procedures for reporting and monitoring is one fundamental tactic. Automated systems have the ability to track domain name registration patterns that may indicate DNS abuse, and protocols for reporting questionable actions can help ensure prompt intervention [41]. To confirm security and ensure that systems have not been compromised, regular audits of DNS setups and domain registrations are also necessary [42] .

1. **Monitoring and Reporting**
    - Implementation: Use automated systems to monitor the registration of domain names for patterns that may indicate DNS abuse [41]. Establish procedures for reporting activities to authorities or cybersecurity organisations [42].
2. **Security Awareness Training**
    - Implementation: Develop training programs for users and IT staff with a focus on recognizing phishing attempts, practicing browsing habits, and understanding DNS security.
3. **DNS Security Extensions (DNSSEC)**
    - Implementation: Deploy DNSSEC to ensure the integrity of DNS data. This involves signing DNS records to protect against modifications and DNS spoofing.
4. **Multi-Factor Authentication (MFA)**
    - Implementation: Enforce multifactor authentication (MFA) for domain registrars and interfaces used to manage DNS [41]. This adds a layer of security beyond passwords, helping to prevent unauthorised domain transfers or alterations [43].
5. **Blacklisting and Takedown Services**
    - Implementation: Collaborate with cybersecurity firms to identify and blacklist domains engaged in malicious activities. Establish response teams dedicated to taking down domains involved in DNS abuse.
6. **Collaboration**
    - Implementation: Foster collaboration among internet service providers (ISPs), domain registrars, governments, and cybersecurity organizations. Share intelligence and best practices to collectively enhance defense against DNS abuse

[44].

7. **Regular Audits**

   - Implementation: Conduct security audits of domain registrations and DNS configurations to verify their security and ensure they have not been compromised [45].

8. **Machine Learning**

   - Implementation: Using AI and machine learning algorithms to analyse patterns in DNS traffic and proactively predict instances of DNS abuse [41]. This proactive approach enables the identification of threats before they materialise [46].

9. **Geo-Blocking and 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 [47].

10. **Enhanced Domain Validation Procedures**

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

Each of these strategies plays a crucial 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.

2.9 Summary and Synthesis

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

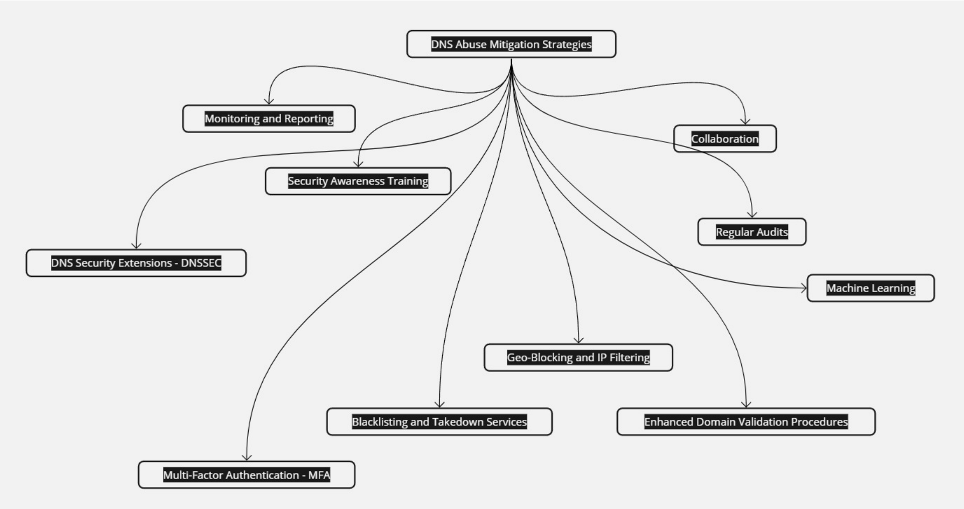
DNS Abuse Mitigation Strategies
Monitoring and Reporting
Collaboration
Security Awareness Training
Regular Audits
DNS Security Extensions - DNSSEC
Machine Learning
Geo-Blocking and IP Filtering
Blacklisting and Takedown Services
Enhanced Domain Validation Procedures
Multi-Factor Authentication - MFA

Figure 2.4: Future dangers of DNS abuse

DNS Abuse	User Harm	Mitigation Strategy	Reasoning	Transparency Aspect
Phishing	Identity Theft, Financial Loss	Security Awareness Training, Enhanced Domain Validation Procedures	Training helps users recognize phishing attempts. Validation prevents registration of mimic domains.	Increases awareness and scrutiny during domain registration.
Confusable Domains (Typosquatting)	Unauthorised Account Access	Enhanced Domain Validation Procedures, Regular Audits	Prevents Registration of Similar Domains. Audits ensure compliance.	transparent domain registration process.
Domain Hijacking	System Compromise, Data Breach	Multi-Factor Authentication (MFA), Regular Audits	MFA secures domain management. Audits verify security measures.	Accountability in domain management.
Botnets	Malware Distribution	Collaboration,Machine Learning	Intelligence Sharing identifies botnet activities. AI predicts the formation of botnets.	Shared responsibility and proactive detection.
Fast Flux Hosting	System Infections	Blacklisting and Takedown Services, Geo-Blocking	Rapid response to malicious domains. Restrict access from risky regions.	Responsive and transparent threat management.
Domain Generation Algorithms (DGA)	Malware Distribution	Machine Learning, DNS Security Extensions (DNSSEC)	AI detects abnormal patterns. DNSSEC prevents spoofing.	Integrity and trust in DNS data.

Continued on next page

DNS Abuse	**User Harm**	**Mitigation Strategy**	**Reasoning**	**Transparency Aspect**
IoT Vulnerabilities	Unauthorised Access, Data Breach	Security Awareness Training, Collaboration	Educates on security practices. Collaboration on best practices.	Open exchange of knowledge and efforts.
Infrastructure Attacks	DDoS Attacks, System Downtime	DNSSEC, Collaboration	Protects DNS data integrity. Sharing of threat intelligence.	Collective action strengthens the DNS infrastructure.
Deepfakes and AI	Identity Theft, Misinformation	Security Awareness Training, Monitoring	Recognising Phishing. Monitor AI threats.	Vigilance and prompt threat reporting.
Cloud Computing Vulnerabilities	Data Breach, Unauthorised Access	Regular Audits, Enhanced Validation	Secure DNS settings in cloud services. Prevents exploitation.	Framework for secure domain use in cloud.
Mobile Device Exploitation	Unauthorised Access, Financial Loss	MFA, Security Awareness Training	Secures account access. Raises awareness of threats.	Mobile security awareness and protection.
Cryptocurrency and Blockchain Exploitation	Financial Theft, Account Compromise	Enhanced Validation, Collaboration	Prevents fraudulent domain registrations. Collaboration on threat intelligence.	Security registration and defence of domains.
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 Their Impact on Users

Finally , This chapter has examined all aspects of DNS abuse, the various forms, the serious harm it does, as well as potential future threats and new trends. To create efficient regulations and countermeasures, it is essential to understand the extent and consequences of DNS abuse. The conversation emphasised DNS's vital function in the digital ecosystem as well as its susceptibility to abuse.Significant progress towards resolving these issues has been made by organisations like the DNS Abuse Institute and ICANN, as well as developments in DNS privacy and security technologies like DoT and DoH. However, as new technologies are incorporated into the equation and the threat environment changes in sophistication, it becomes increasingly important to adopt alert, flexible, and cooperative strategies.

The mitigation techniques and best practices discussed in this chapter provide a roadmap for mitigating DNS abuse. Every tactic contributes to a defence mechanism, from advanced technology solutions and improved methods for validation to monitoring and reporting. It is impossible to overestimate the value of cooperation, regular checks, and the application of cutting-edge technologies to anticipate and stop DNS abuse. After analysing the data, it is evident that a team effort is needed to comprehend, track, and mitigate DNS abuse. A complex strategy that integrates multiple techniques and encourages collaboration across industries is required instead of a single, insufficient strategy. Our approaches to preserving the integrity and security of the DNS and, consequently, the larger internet infrastructure must adapt as does the digital environment.

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

3 State of the Art

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

3.1 Current Strategies and Their Effectiveness in Relation to DNS Abuse

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

3.1.1 Advanced Mitigation Strategies

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

3.1.2 Evaluation of Transparency

The trends in DNS abuse had declines among some categories, such as botnets, malware, phishing, and spam. Much of this decline could be attributed to the multi-pronged approaches that ICANN itself launched around data analysis, community tools, and enforcement of registry and registrar obligations. While continuing to be slow, adopting organisations did so under the compulsion of situations that left them no choice but to use the 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. In addition, there is privacy because DNS queries are able to inadvertently expose user behaviours, thus the basis for initiatives such as Query Name Minimisation to protect user privacy. The challenge always remains for these algorithms and technologies: how to maintain vigilance on the abuse of a domain name system, adding privacy without any loss in efficiency.

3.2 Emerging Trends in DNS Abuse

The 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 multi-pronged approaches that ICANN itself launched around data analysis, community tools, and enforcement of registry and registrar obligations. [?] While continuing to be slow, adopting organisations did so under the compulsion of situations that left them no choice but to use the 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 behaviors. One such move to enhance user privacy is the Query Name Minimization. The main concern has been how to remain vigilant against DNS abuses while improving privacy without impairing service efficiency.

3.2.1 Evolving New Forms of DNS Abuse

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

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

3.2.2 Predictive Measures and 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 the damage and losses related to the 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 accounts which are maliciously generated 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 to the communication infrastructure and the corresponding IP addresses, through either suppression or sinkholing in the context of botnets and the use of Domain Generation Algorithms (DGAs) that direct botnet traffic. [?] Most specifically, sinkholing is an authoritative measure that directs traffic from abusive domains to harmless servers and allows studies to be conducted on the sources of traffic and the extent of compromise. Compliance with legal and contractual requirements further underscores the actions of registrars and registries against DNS abuse, ensuring that their actions in mitigation are within the context of the ICANN agreements and local laws.

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

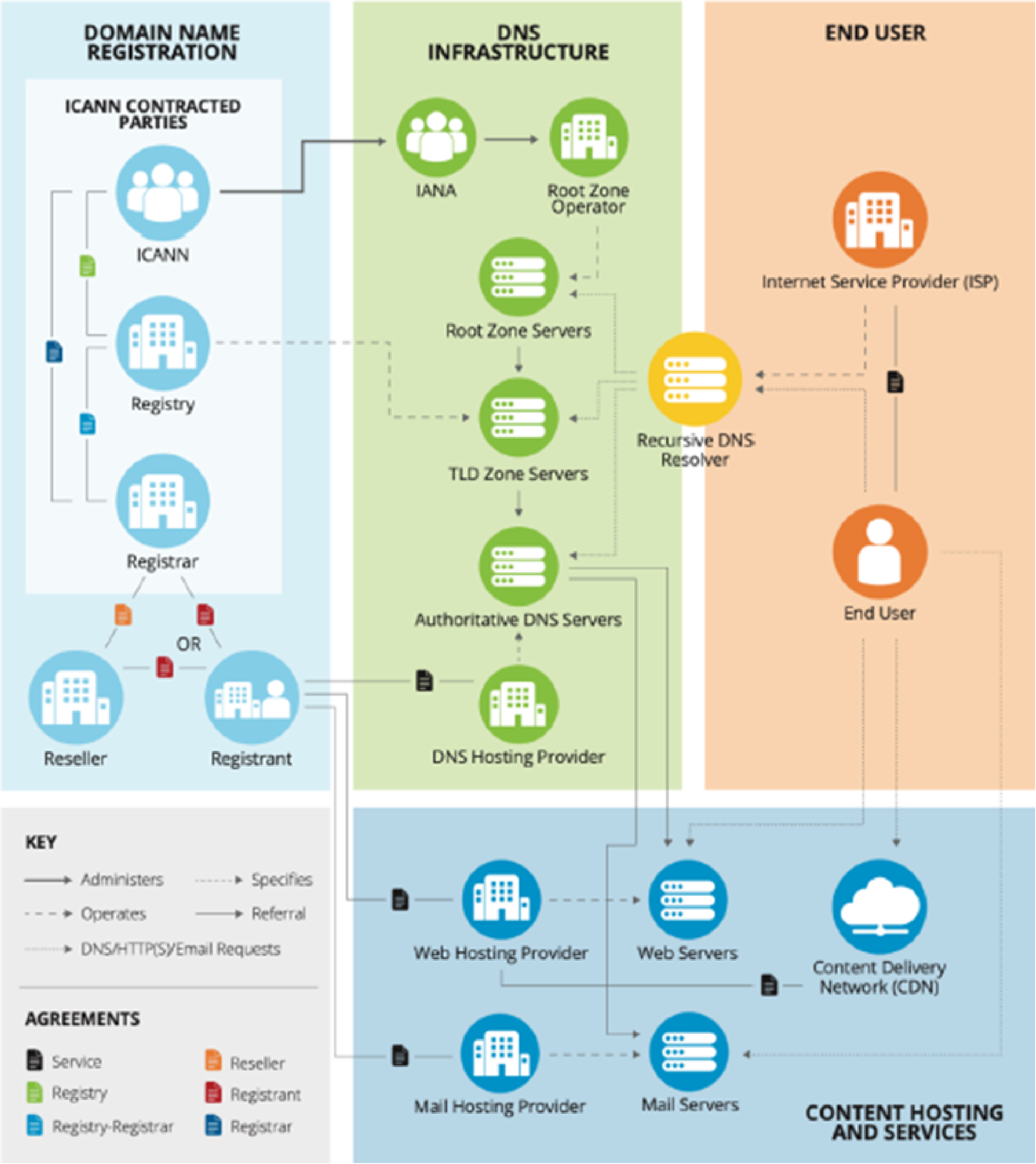

Figure 3.1: Conceptual Diagram of the DNS Ecosystem Portion Contractually Related to ICANN (image courtesy of Verisign and originally published in SSAC 115)

3.3 Technological Advancements

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

3.3.1 Role of AI and Machine Learning

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

In summary, leveraging AI and machine learning for DNS abuse mitigation signifies a transformative shift in cybersecurity practices. The strategic application of these technologies substantially strengthens the DNS system's defence against a wide array of cyber threats, marking a significant advancement in the ongoing battle against digital abuse.

3.3.2 DNS Abuse Transparency Challenges with AI and Machine Learning

AI and machine learning can help improve DNS abuse mitigation, but experts need to fix problems by being clear. People are worried about understanding why complex systems make choices because of the "black-box" part. 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 needing to write down what data was used for training, telling others about the things that affect choices, and explaining how models change to face new risks. It is still hard to find the right balance between the complexity needed for good threat detection and the openness needed for blame.

3.4 Case Studies and Real-World Applications

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

1. **Case Study 1: XYZ Corporation**

   In this case, the study completely analyses one specific company, XYZ Corporation, as an example of DNS abuse in the real-world environment and analyze all details through figures, graphs, and charts. This abuse of DNS took place as a prolonged campaign against XYZ Corporation, a multinational technology conglomerate [?]. Attackers used weaknesses in the company's DNS infrastructure to perform various malicious activities, including domain hijacking, DNS tunneling, and DDoS attacks. A timeline graph was also prepared to see the scale of abuse and how attacks progressed with each event that occurred in the organisation, as shown in Figure 3.2.

   The relationship between this correlation raises questions about the attackers' understanding of the inner workings of the firm, as well as insider threats. A closer

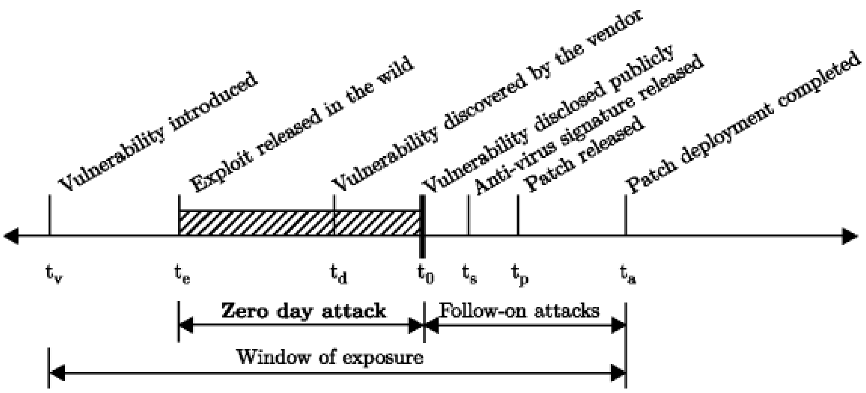
Vulnerability introduced
Exploit released in the wild
Vulnerability discovered by the vendor
Vulnerability disclosed publicly
Anti-virus signature released
Patch released
Patch deployment completed
t_v
t_e
t_d
t_0
t_s
t_p
t_a
Zero day attack
Follow-on attacks
Window of exposure

Figure 3.2: Timeline of DNS Abuse Attacks on XYZ Corporation

analysis of the DNS abuse types employed by such offenders revealed that domain hijacking was common [?]. Figure 3.3 shows how various DNS abuse techniques were used in the case of XYZ Corporation, and domain hijacking was significantly higher than all other combined methods.

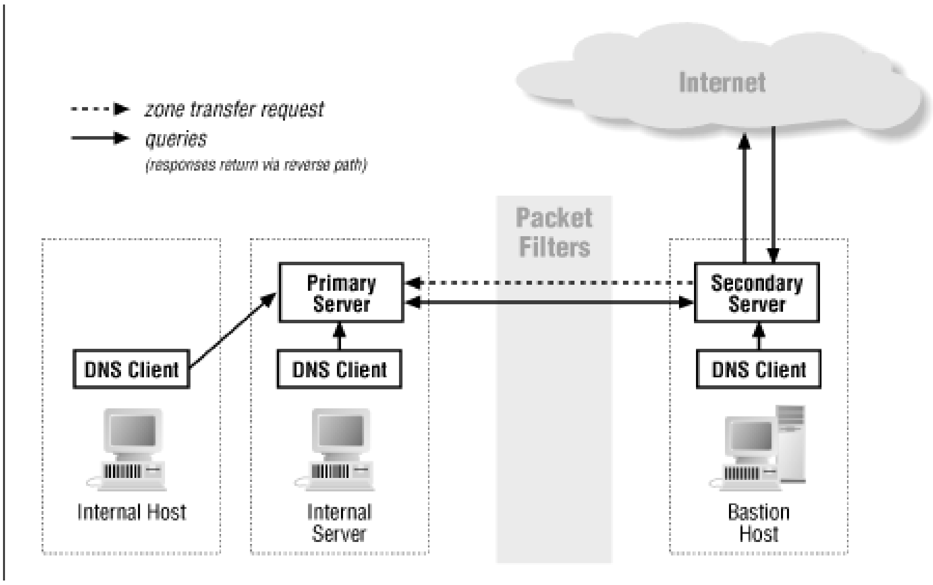

Figure 3.3: Distribution of DNS Abuse Techniques Against XYZ Corporation

There is a domain hijacking technique where attackers may effectively take control over a company without authorisation; domain hijacking is one of the major threats to the organisations that are affected. The figure shows that strong security is key to preventing unauthorised access to domain registration accounts; favouring multifactor authentication is the way to keep these attacks away [?]. This case study sheds light on the subtleties of DNS abuse as it targeted XYZ Corporation, showing the importance of understanding and dealing with an unpredictable cyber threat environment. Figures, graphs, and graphs serve to illustrate safeguard attack procedures and give credence to the notion that an all-encompassing cybersecurity strategy is integral to mitigating DNS abuse in the digital landscape of the networked world of our day.

2. Case Study 2: OilRig DNS Tunneling Attack

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

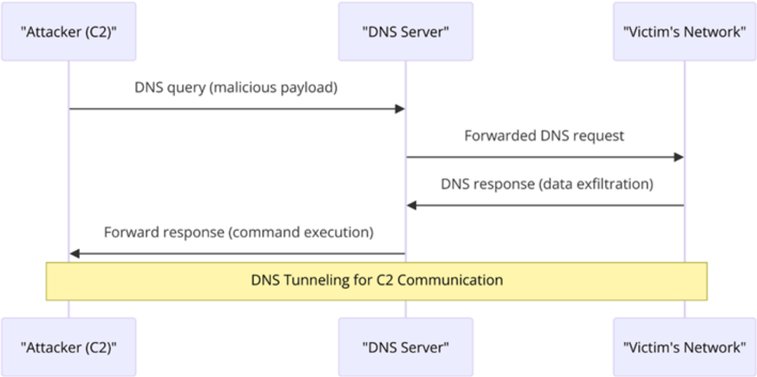
"Attacker (C2)"
"DNS Server"
"Victim's Network"
DNS query (malicious payload)
Forwarded DNS request
DNS response (data exfiltration)
Forward response (command execution)
DNS Tunneling for C2 Communication
"Attacker (C2)"
"DNS Server"
"Victim's Network"

Figure 3.4: DNS tunneling communication between the attacker's command and control (C2) infrastructure and the victim's network

3. Case Study 3: SUNBURST Use of DGAs

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

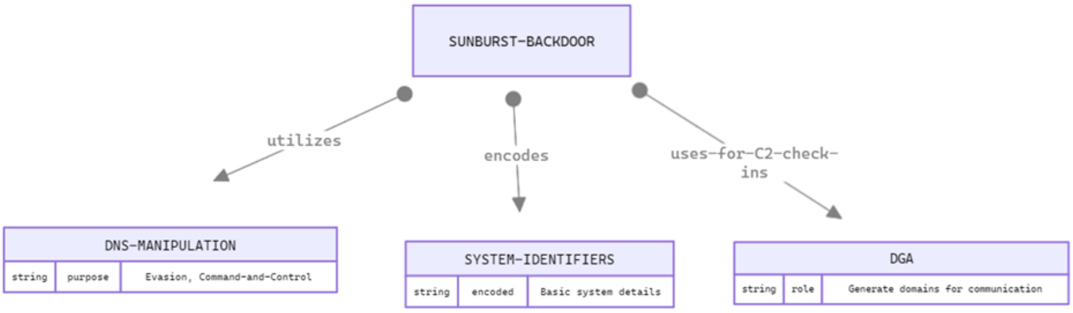

Figure 3.5: SUNBURST backdoor's utilization of DGAs and its associated components

4. **Case Study 4: Fast Flux Techniques** The presence of several C2 domains related to the Smoke Loader malware family using Fast Flux techniques only further underscores the difficulties associated with the tracking and eradication of DNS-enabled threats. [?].The major takeaway in the rapid rotation of IP addresses of this method points to the dynamism of strategies used in communications by malware, thus improving the means of defence by cybersecurity. [?]

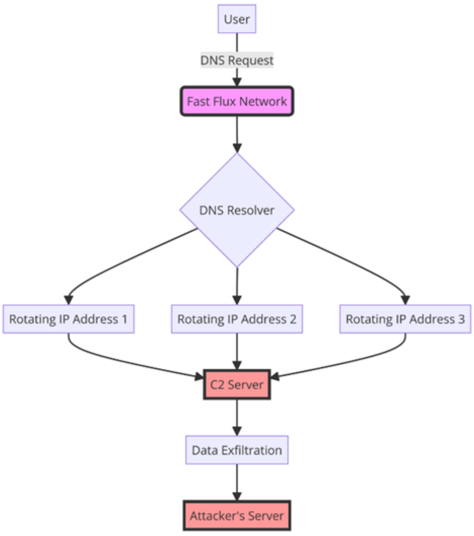

Figure 3.6: The usage of Fast Flux techniques by the Smoke Loader malware family for dynamic C2 domain communications

5. **Case Study 5: Malicious Newly Registered Domains (NRDs)**

   The malicious NRDs opportunistically crafted in the milieu of the pandemic expose how threat actors leverage current events for engineering targeted attacks. [?] From domains that mirror COVID-19 information resources to those faking government relief programmes, the evolution of such attacks reflects a calculated approach to exploiting public interest and vulnerabilities. [?]

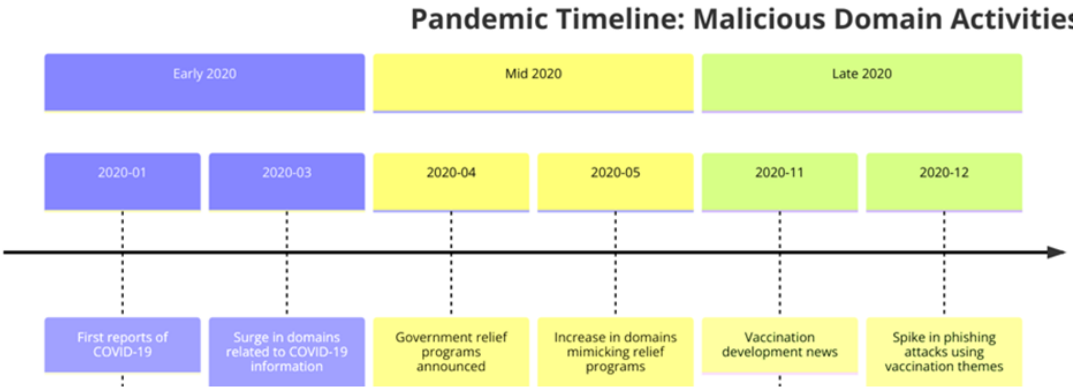
Pandemic Timeline: Malicious Domain Activities
Early 2020
Mid 2020
Late 2020
2020-01
2020-03
2020-04
2020-05
2020-11
2020-12
First reports of COVID-19
Surge in domains related to COVID-19 information
Government relief programs announced
Increase in domains mimicking relief programs
Vaccination development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

Figure 3.7: 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 programs, and subsequently enlisting vaccine distribution. Several of them, in fact, employed sophisticated tools like MFA pretending as U.S. Federal Trade Commission and brands such as Pfizer and BioNTech, to steal credentials. where it emphasized that there was a 530% surge in vaccine-related phishing attempts and a 189% hike in attacks on pharmacies and hospitals from December last year to February this year. Advice was given for individuals and organizations that include being cautious in email and website dealings, stepping up security awareness training, as well as adopting multi-factor authentication.

Since January 2020, a total of 69,950 COVID-19 related phishing URLs, of which 33,447 are specifically dedicated to COVID-19. The data has been normalized in such a way that the peak of each topic is at 100%. 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.

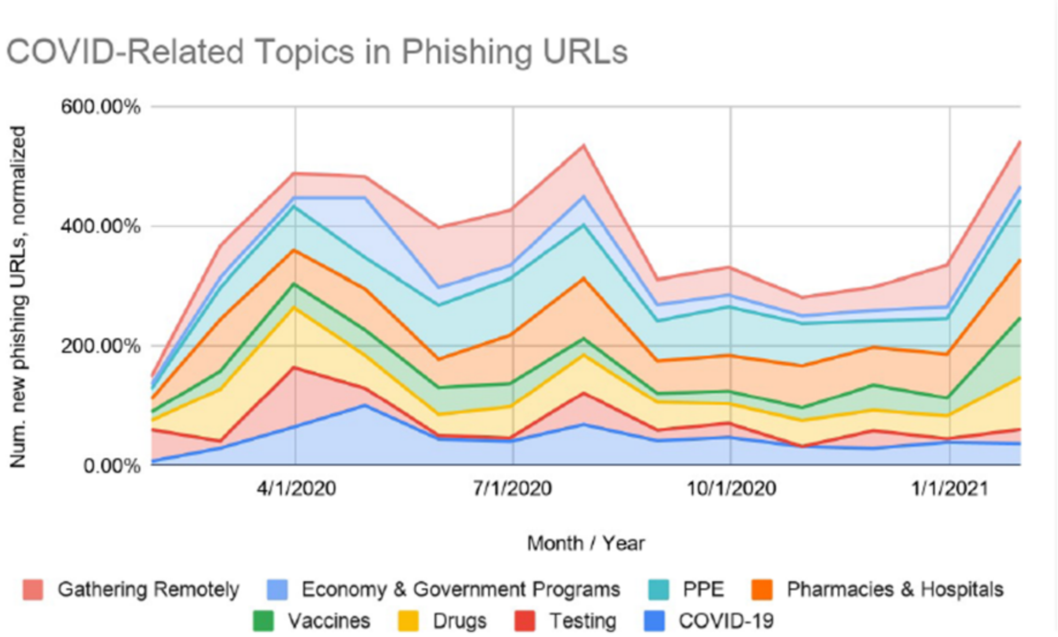

Figure 3.8: Development trends in the majority of COVID-19-related phishing content hosting sites during the period from January 2020 to February 2021.

It is evident to state that a major chunk of COVID-19-themed phishing pages targeted leading brands for phishing business credentials, such as Microsoft login, Webmail, and Outlook login. For example, about 23% of these phishing URLs posed to be Microsoft login pages. This threat has particularly highlighted the shift towards remote working in the pandemic and, hence, magnified the relevancy of these attacks as one of the foremost methods to be undertaken by cybercriminals.

This thus clearly indicates a situation whereby the attackers set up websites frequently for

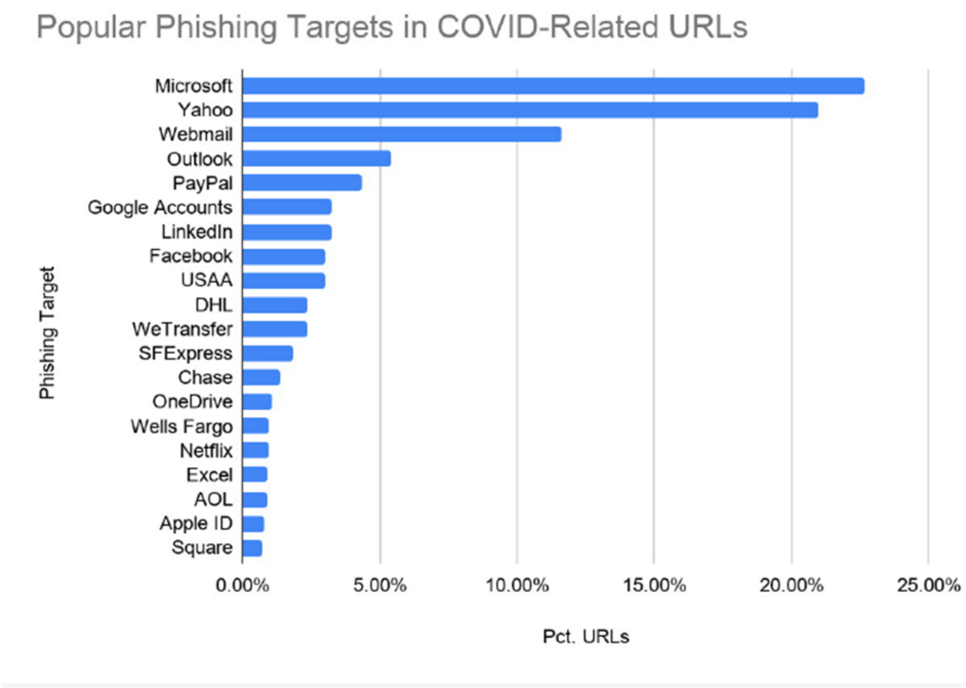

Figure 3.9: Top spoofed websites in COVID-themed phishing attacks (global), where the percentage in each column is the percentage of phishing volume per site and category.

COVID-19 themed phishing attacks. Many of these phishing pages are found on sites created less than 32 days meaning these sites are launched with specific purposes in view of these imminent attacks. The strategy avails attackers to customize their messages and URLs to the state-of-the-current pandemic trends, indicating the dynamism behind such cyber threats.

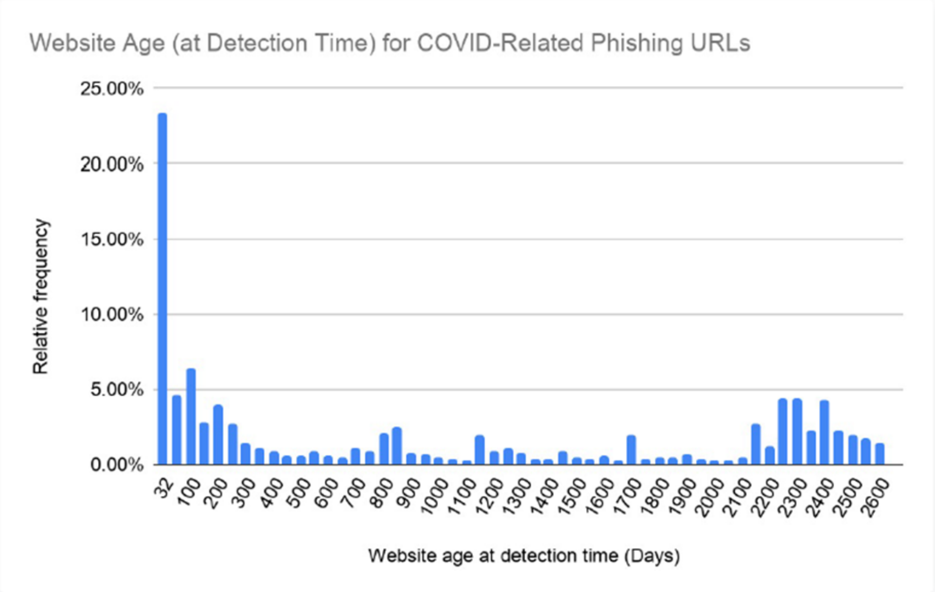

Figure 3.10: Statistic of lifespan distribution of COVID-19-related phishing content hosting sites when the sites are reported .

3.5 Challenges and Future Directions

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

3.5.1 Identification of Current Challenges

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

3.5.2 Discussion on Future Research Directions and Technologies

When planning to mitigate the DNS abuse in the future, discussing new research ideas and upcoming technology is crucial. The constantly changing state of Internet threats requires us to continually create new things. This is so people can stay one step ahead of the bad people. Future work on DNS abuse needs to start by building better tools. These can help to address how bad guys on the Internet keep changing their tricks [?]. This means that we need to look at more complex AI and machine learning tools that can understand the details of web traffic. This will make the results more accurate and stop wrong signals from being sent. Moreover, there is a rising need to use blockchain tech to make domain registration safer and stop any bad or harmful changes, as it provides decentralised domain name resolution unlike traditional DNS systems, which rely on a central authority to resolve domain names, a Blockchain DNS operates on a network of distributed nodes in which each node has a copy of the entire blockchain ledger, so it can independently verify and resolve domain name requests, which not only makes the system more resilient to attacks but also prevents censorship and control by a single entity. [?]. People should have easy methods to report DNS abuse. This will make sure everyone knows about dangers [?]. Working together in the world is very important because computer dangers go beyond borders. So everyone in the world needs to work together.

3.6 Conclusion

DNS abuse continues to be a big issue. Present plans, while sometimes useful, require constant adjustment and getting better. It's key to have solutions for fixing issues available. This helps to build trust and work well with those involved. Abusing DNS in new ways brings fresh issues that require clever solutions. AI and machine learning can help find things, but we need to show how they work better so that people can keep bad people under control. Learning from real-life situations teaches us a lot about good and bad ways of being open. This helps us create the best methods for our business. There are still issues with showing and stopping DNS abuse while trying to find new ways to mitigate this DNS abuse. People need to continue learning and working as a team. People should focus on better technology, joining forces with other nations, and using common methods of sharing information in the future. As the internet changes, we must stay active and work together to stay ahead of bad people who want to hurt us.

3.7 Summary of Findings

The study on DNS abuse looked at current ways, checked new trends, talked about tech advancements, and explored real examples in life. The search for ways in the plans to mitigate DNS abuse showed the value of clear communication and honesty in building trust with the community. People are finding new ways to abuse the DNS system. Researchers have to keep making new things, so they don't get caught by changing dangers. Improvements in technology, especially with artificial intelligence and learning machines, showed how automation can make it easier to spot dangers. But it also made things harder to understand, and this needs careful attention. Examples from real life showed what did and did not work in making DNS abuse clearer. These provided essential advice for the business. Issues with making things clear and stopping wrong actions were found. This shows how important it is to continue learning and working with others. In the future, discussing issues and future plans will show the need for creative studies, help from other nations, and common ways to share information.

4 Draft

4.1 Confusable Domains

4.1.1 Identification and Examples of Targeted Domains

The choice of such domains to target and outsource depends on many factors, each with its implications on the business strategy, marketing, and observance by law. 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 to try to negotiate the hurdles of the digital market and to protect rights through intellectual property.

To navigate these complexities effectively, it is essential to consider several key factors.

- **Commercial Appeal:** High commercial appeal domains are lucrative targets due to the extremely high possibility of attracting a large traffic flow, with potential revenue generation. Such names are easy to remember, short in length, and directly linked to products or services under some category that is searched most frequently.[**?**]

- **Keyword Relevance:** Targeted domains have a certain relevance that holds the keyword itself. These domains are ranked higher in search engine outputs and attract organic traffic, making them a useful tool for businesses aiming to align with the primary keywords used by their target customers.

- **Similarity to Well-known Trademarks:** This refers to the practice of registering domains that are similar or confusingly like existing trademarks—known as cybersquatting. This can lead to confrontations with the rightful trademark holders. Trademark law aims to prevent consumer confusion and protect the goodwill associated with the trademark, particularly in disputes over domain infringement.

4.1.2 Real-life examples

- **Cybersquatting :** is securing domain names that are the same as or in the likeness of trademarks or brand names, with the intent to sell them at grossly marked-up prices back to the true owner. Among the most notorious examples are several court battles based on the purchase of "nissan.com" and "nissan.net" by a person named Nissan, who owned Nissan Computer Corp many years before Nissan Motors tried to acquire it. This case highlighted tension between the protection of trademarks and individual's interests in using their names for domain name purposes as well as it underscores the challenges of domain name registration and trademark protection in the digital age where domain names closely resemble established trademarks, potentially leading to consumer confusion and dilution of trademark's value. [?]

- **Typosquatting- URL hijacking :** it deals with the registration of misspelled variants of well-known domain names for the mere purpose of capturing traffic from users who tend to make mistakes in typing a URL. They could register "goggle.com" instead of "google.com" which was used to direct users to a site that bombarded their browsers with pop-ups and ads , leading to malware infections as that site was designed to capitalize on accidental misspellings or phishing attempts that tricked users into visiting. [?]

- **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 otherwise be described as using legal or dispute resolution mechanisms to try to force people from their domains. [?]

  An RDNH was claimed in a UDRP action against "groovle.com," in which the domain was purported to be too close to Google's trademark. However, since the domain was used for another search engine, it was deemed legitimately used and not to have infringed on Google's trademark or registered in bad faith. [?]

- **Homograph attacks:** are those cases in which people have registered domains using characters that kind of look similar to those used on legitimate sites for instance, using a homographic character to make 'Google.news' appear as 'google.news'. This technique has been followed by fraudsters who are now imitating various Google domains for phishing purposes. The group said it reported similar flaws with applications such as Signal and Telegram, where homograph attacks deceived the user to visit harmful sites by using Unicode in domain names to look like famous brands, including phishing attempts on MyEtherWallet and GitHub users. [?]

4.1.3 Real-life Mitigations

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

- **Cloudflare's Zero Trust Services Approach :** Protection from this problem of newly created phishing websites is given by Cloudflare itself with its protection in the form of Zero Trust services, finding these websites, and blocking confusable domains. Cloudfare zero-trust rules can be enforced using Cloudfare Gateway in a way that they deny access to these illegitimate domains. In such a way, corporate networks are supposed to be secured from phishing attempts that take advantage of human trust in well-known brands. [?]

- **Swift-URL-SpoofCheck Initiative:** On this open source initiative hosted on GitHub, a domain renderer has been released for the WebURL format defined according to the algorithmic rules established by IDN spoof checking in Chromium has been released. This tool intends to provide the user with an additional form of safety from domains that look confusingly like known-good domains by integrating most but not all the rules that Chromium uses in the label verification process. It includes functionality to identify potential spoofs and visualise how what appear to be valid domains could be deceptive. [?]
- **IDN Handling of Google Chrome:** Google Chrome enforces an IDN (Internationalized Domain Names) policy to determine which form the Unicode or punycode form a domain label should be displayed in. The domain label is tested whether it has mixed script, invisible characters, or visually confusable characters, and whether it is actually validly converted into 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 further offers comprehensive warnings to secure URLs that appear to be an imitation of already known web pages. [?]

In addition to what I mentioned above, let us look at the most popular mitigations used world-wide :

1. Deployment of DNS Security Extensions (DNSSEC): DNSSEC introduces an additional security layer to the DNS query and response mechanism, helping protect against DNS spoofing attacks that often accompany confusable domain strategies.
2. Typo-squatting Detection Tool: Tools such as DNStwist and URLCrazy are used to offer organizations similar domain names so that they can either secure these domain names in advance or file litigation for the same.
3. Anti-Phishing Working Group (APWG): It is a pool for stakeholders to share intelligence, trends and best practices regarding phishing and similar threats associated with confusable domains in which mitigation is carried out in collaboration action between cybersecurity entities and domain registrars, as it allows sharing of threat intelligence with respect or cancelling out the holding of malicious domains.

4.1.4 Collaboration Among Registrars, Registries, and DNS Collaborators

This collaboration should be achieved with DNS registry, registry and collaborators. In that way, they can boost common resources and intelligence that can guide in making the internet more secure and resilient. This strictly falls within the remit of registries and registrars acting in collaboration to put in place such stringent registration policy with procedures for verification, checking against mimicking existing trademarks or even popular domain names.

In this way, the collaboration can even manifest itself via the sharing of sensitive data with regards 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 demands that registrars, registries, and DNS collaborators work in a common effort. This is due to the increasing level of threats and the shared responsibility of all the actors involved in the DNS ecosystem. [?] To put this into perspective, here are some examples:

1. Recent changes in the contract from ICANN's contracted parties have imposed on registrars and registries new specifications to define DNS abuse, together with clear requirements for the actions to be taken by such parties immediately actionable evidence of abuse is received. This is a major step towards establishing more clarity about the roles that may be played by these different stakeholders in addressing the matter of DNS abuse and ensuring there is a common approach to redress. [?]

2. Approved new obligations of ICANN's contracted parties have been by the community itself further to mitigate DNS abuse, thereby demonstrating the will of the community to come together to address the issues of DNS abuse. [?]

3. Efforts like NetBeacon, with the support of the DNS Abuse Institute, are being rolled out to reduce friction in reporting and mitigating DNS abuse. This service solves the current complexities and quality standards associated with the reporting of DNS abuse as it makes the work easier for the registrars, ultimately narrowing down their scope to the relevant and evidenced report as well as it underlines the need for cooperation among registrars, registries, and other DNS stakeholders. This is what is capable of saving the Internet and safeguarding at the same time the credibility and confidence of DNS. [?]

4.1.5 Techniques for Mitigating Confusable Domains

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

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

1. Registry-Level Measures: Domain registries can implement checks to prevent the registration of domains that are too like existing trademarks or brand names, using algorithms to detect variations and misspellings closely resembling protected names. [?]
2. Trademark Protection Programs: Services like the Trademark Clearinghouse (TMCH) offer mechanisms for trademark holders to protect their rights by receiving notifications when someone attempts to register a domain matching their trademark. [?]
3. Automated Monitoring and Reporting: Automated systems can continuously monitor domain registrations for names that closely resemble known trademarks or brand names, enabling rapid detection and legal action against infringers. [?]

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

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

4.1.6 Technical and Operational Feasibility

The technical feasibility of these techniques varies. Registry-level measures and trademark protection programmes are highly effective, but require cooperation and standardisation across different legal jurisdictions. Automated monitoring is technically feasible and can be implemented at scale but requires resources for continuous operation and legal follow-up. Browser-level defences are among the most directly impactful, protecting users at the point of access, yet they depend on browser vendors' willingness to implement and maintain these features, and collaboration frameworks play a crucial role in mitigating confusable domains. Initiatives such as the Trademark Clearinghouse (TMCH) facilitate cooperation between trademark holders and domain registries. Meanwhile, organisations such as the Anti-Phishing Working Group (APWG) and the Internet Corporation for Assigned Names and Numbers (ICANN) work toward broader solutions that encompass both non-IDNs and IDNs.

4.1.7 Transparency in Mitigation Efforts

Transparency in the mitigation of confusable domains plays a pivotal role in the broader strategy to secure the Internet against phishing attacks, trademark infringement, and other malicious activities. This concept entails the practices adopted by domain registries and registrars in identifying potentially malicious domains that mimic or closely resemble legitimate ones, and the extent to which these entities disclose identified confusable domains to the public. One of the primary methods to improve transparency involves the publication of lists of confusable names by registries and registrars. These lists typically include domains flagged for their similarity to existing domain names, potentially infringing trademarks, or those that could be used for malicious purposes. The publication aims to alert the internet community, including businesses and end-users, about possible threats, thereby fostering a proactive approach to domain name security. Here is how transparency can be applied to each of the mitigation techniques described:

- **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.
- **Swift-URL-SpoofCheck Initiative:** Transparency in this open-source project is inherent through its availability on GitHub, allowing users and developers to scrutinize, contribute to, and understand the tool's underlying logic. The initiative should continue to provide comprehensive documentation on how it integrates Chromium's

IDN spoof-checking rules and the rationale behind excluding certain steps. This openness encourages community engagement and continuous improvement of the tool.

- **IDN Handling of Google Chrome:**Google's approach to displaying domain names in Unicode or punycode based on their potential for deception benefits from transparency about its IDN policy. Detailed explanations of the checks performed (e.g., mixed script detection, invisible characters) and how decisions are made improve user understanding and awareness of potential threats. Furthermore, publishing information on how users can report misclassified domains or suggest improvements to the IDN policy can further empower users and foster a safer Internet environment.
- **Deployment of DNS Security Extensions (DNSSEC):** For DNSSEC to effectively improve trust in the DNS, the processes for securing DNS records and verifying DNS responses should be transparent to DNS administrators and end users. Providing educational resources and clear guidelines on how to implement DNSSEC can help demystify this complex security layer and encourage its widespread adoption.
- **Typo-squatting Detection Tools:** The effectiveness of tools like DNStwist and URLCrazy in helping organizations identify potential confusable domains relies on transparency about how these tools generate similar domain names and the criteria used for detection. Openly sharing updates, methodologies, and case studies can help organisations better understand how to use these tools proactively.
- **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 the 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 Programs: Services such as those from a Trademark Clearinghouse (TMCH) should operate with full transparency regarding the

conductance of verification, matching, and notification. This can help trademark holders by demonstrating transparent guideline procedures that show both the rights of trademark holders and what needs to be done to effectively protect their brands.

3. Automated Monitoring and Reporting: The automated monitoring systems must be built with such predefined criteria, algorithms, and thresholds that potentially support the involvement of stakeholders. It also makes sure that the brand owners are aware to what extent his trademarks are protected, and thus allows for some parameters within such services making the monitoring more successful.

- **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: A good web browser should play the most critical role in defending against IDN homograph attacks. Browsers must document, provide, and communicate their defence mechanisms in a clear and plain manner to users. For instance, they should indicate when a domain is being displayed in puny code or the scenarios under which their warnings are triggered. This can only give a user assurance if there is transparency as a rationality measure for them in such defence measures to be able to rationalize the triggering of any warning and know what action to take.

    3. Collaborative Blacklisting and Shared Threat Intelligence: Processes for the addition of domains to blacklists and criteria that determine whether a domain is to be considered malicious should be examined. Organisations that put in place an intelligence sharing regime also need to have some rules on data submission and validation and data disposal from blacklists. Transparency in these processes can best ensure that blacklisting is done fairly and accurately and allows the right of appeal, improving trust in collaborative security.

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

4.1.8 Benefits of Transparency

The benefits of transparency in the context of confusable domains are multifaceted. Firstly, it promotes accountability among domain registrars and registries, encouraging them to actively participate in the detection and mitigation of confusable domains. Second, transparency acts as a deterrent to malicious actors who might otherwise exploit the anonymity afforded by a lack of public scrutiny. Third, by making such lists public, registries and registrars can empower businesses and trademark owners to take timely action to protect their brands, such as through legal mechanisms or domain purchases. Furthermore, transparency supports community-based mitigation efforts, where cybersecurity researchers and the wider community contribute to identifying and neutralizing threats. This collaborative approach leverages the collective expertise of the cybersecurity community, enhancing the overall effectiveness of mitigation strategies.

4.1.9 Drawbacks and Security Concerns

However, the publication of confusable domain lists is not without its drawbacks and security concerns. One major concern is that making such lists public could inadvertently provide a roadmap for malicious actors, highlighting potential targets for exploitation. This could lead to a situation where attackers use the information to refine their strategies, for example, by registering domains not yet identified or listed, thereby staying one step ahead of mitigation efforts. Another concern revolves around the risk of false positives, where legitimate domains are mistakenly flagged as confusable. This could harm businesses and individuals whose domain names are wrongfully listed, potentially leading to unwarranted scrutiny, legal challenges, and reputational damage. Moreover, the debate between transparency and security also touches on the effectiveness of disclosure in preventing attacks. While transparency aims to preemptively combat threats, there is an argument that the sheer volume of domain registrations and the dynamic nature of domain abuse may limit the practical utility of such lists to end-users and businesses.

4.1.10 Analysis : Feasibility and 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. Monitoring Punycode Registrations: Feasible; This option is feasible and will require mainly the use of existing technology and cooperation that could be initiated with little difficulty between relevant stakeholders.

3. Blacklisting and Threat Intelligence Sharing: Moderately Feasible; Since agreement

could be reached on shared platforms and protocols, but they imply strong cooperation and trust among such diverse entities, which is unlikely to be developed fast.

4. Registry-Level Measures: Not Feasible; this would require very heavy coordination and agreement on standards across diverse jurisdictions and registries, very complex in nature and long-drawn.
5. Trademark Protection Programs: Moderately Feasible; They are well-functioning processes under such adequate structures like TMCH and can be learnt while proceeding with experience, but likely to face legal and operational issues.
6. Browser-Level Defences: Not Feasible; While this is technically feasible, it seems rather infeasible soon that user practices will become uniform across all web browsers and that all users will be well trained in various security practices.
7. Cloudflare's Zero Trust Services Approach: Feasible; since well-architected infrastructure and broad adoption have made Cloudflare zero trust rules simple and effective to deploy, with a balance of security and operational efficiency without seismic root and branch changes.
8. IDN Handling of Google Chrome and Browser-Level Defences: Feasible; Given that Chrome today has an enormous user base and that the groundwork for stopping homograph attacks already exists, it stands to reason that a solution is reasonably possible, meaning not too difficult, within a set timeline, and within the lifespan of any other typical software product.
9. Less feasible options that would introduce some serious friction or are the use of DNSSEC (Domain Name System Security Extension), which is a solution that has a serious implementation downside due to its complexity and the need for stakeholders' absolute timing and synchronisation.

5 Research

5.1 Introduction to Research Methods

5.2 Questionnaire Design and Distribution

5.3 Stakeholder Responses

5.4 Types of DNS Abuse Encountered

5.5 Challenges in Mitigation

5.6 Mitigation Strategies

5.7 Transparency in DNS Abuse Mitigation

5.8 Impact on Relationships within the DNS Ecosystem

5.9 Data and Evidence Acquired

5.10 Analysis of Research Outcomes

5.11 Conclusion

6 Evaluation

7 Conclusion

8 Findings

This document provides a template for the preparation of final year project reports. The objective is to provide clear guidance to you, the students, and also to provide uniformity to the project reports, to facilitate equitable grading. This LaTeX template uses a sans-serif font to aid accessibility..

The font colour for Chapter headings is "Pantone Blue", which is the colour used in TCD documents. The page number appears at the bottom of each page starting at 1 on the first page of the Introduction chapter. If you are not familiar with concepts like styles, captioning, cross-referencing, and how to generate tables of contents, figures etc. in LaTeX, the Overleaf guides are a useful start at:
`https://www.overleaf.com/learn/latex/Learn_LaTeX_in_30_minutes`

8.1 Headings, sections and subsections

Chapters should be divided into appropriate subsections. LaTeX makes the numbering much easier and it is all built in. Headings should incorporate the Chapter number into them as is done here.

8.1.1 Subsection name style

The subsections, if used, should be numbered sequentially within each section. You should really try to avoid using sub- subsections, but if you do they should not be numbered.

8.2 Length of the report

The page margins is set to 2.54 cm top, bottom, left and right. There may be a table or figure for which it is sensible to deviate from these margins, but in general the main text should be formatted within the specified margins. The body of the report should be organised into several chapters. There are a number of chapters that you must have: an introduction; a background or literature review chapter; and a conclusion chapter. The focus of the other chapters will depend on your specific project. Refer to the issued guidelines for the page limit. This limit does not usually include the front matter, references list and any appendices. In other words, from the first page of the Introduction to the last page of the Conclusions chapters must be less than the given limit for MAI. If you exceed these page limits or deviate significantly from this format, you will lose marks.

8.3 Contents of the Introduction

The introduction presents the nature of the problem under consideration, the context of the problem to the wider field and the scope of the project. The objectives of the project should be clearly stated.

8.4 Contents of the background chapter

Bibliography

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

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

[3] D. Tatang *et al.*, "The evolution of dns-based email authentication: Measuring adoption and finding flaws," 2021. [Online]. Available: https://dl.acm.org/doi/10.1145/3471621.3471842

[4] G. Holdmann *et al.*, "Renewable energy integration in alaska's remote islanded microgrids: Economic drivers, technical strategies, technological niche development, and policy implications," 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8801901

[5] 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. [Online]. Available: https://link.springer.com/content/pdf/10.1007/s10922-020-09564-7.pdf

[6] A. Mathew and C. Cheshire, "Trust and community in the practice of network security," 2016.

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

[8] E. I. Medvedskaya, "Features of the attention span in adult internet users," 2022. [Online]. Available: https://journals.rudn.ru/psychology-pedagogics/article/view/31393

[9] 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

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

[11] C. Deccio and J. Davis, "Dns privacy in practice and preparation," *ACM Digital Library*, 2023, accessed: 13/10/2023. [Online]. Available: https://dl.acm.org/doi/10.1145/3359989.3365435

[12] "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

[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] K. Hynek, T. Cejka, A. Wasicek, J. Luxemburk, and D. Vekshin, "Summary of dns over https abuse," *IEEE Xplore*, 2023, accessed: 13/10/2023. [Online]. Available: https://ieeexplore.ieee.org/document/9775718

[15] M. Lyu, H. H. Gharakheili, and V. Sivaraman, "A survey on dns encryption: Current development, malware misuse, and inference techniques," *arXiv*, 2023, accessed: 13/10/2023. [Online]. Available: https://arxiv.org/pdf/2201.00900v1.pdf

[16] "Webinar: Understanding and combating dns abuse - encouraging best practice," *ICANN*, 2023, accessed: 13/10/2023. [Online]. Available: https://features.icann.org/event/icann-organization/webinar-understanding-and-combating-dns-abuse-%E2%80%93-encouraging-best-practice

[17] 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.

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

[19] 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.

[20] B. Edelman, "Typosquatting: Unintended adventures in browsing," *McAfee Security Journal*, pp. 34–7, 2008.

[21] 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."

[22] 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.

[23] 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.

[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.

[26] 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.

[27] K. Fowler, *Data breach preparation and response: breaches are certain, impact is not*. Syngress, 2016.

[28] 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.

[29] J. Saxe and H. Sanders, *Malware data science: attack detection and attribution*. No Starch Press, 2018.

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

[31] CircleID, "A look at dns trends and what the future may hold," https://circleid.com/posts/20201028-a-look-at-dns-trends-and-what-the-future-may-hold/, 2020, accessed: 25/10/2023.

[32] 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.

[33] M. Dooley and T. Rooney, *DNS Security Management*. John Wiley & Sons, 2017.

[34] N. Schick, *Deep fakes and the infocalypse: What you urgently need to know*. Hachette UK, 2020.

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

[36] M. H. Au and R. Choo, *Mobile security and privacy: Advances, challenges and future research directions*. Syngress, 2016.

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

[38] M. Chapple and D. Seidl, *Cyberwarfare: Information operations in a connected world*. Jones & Bartlett Learning, 2021.

[39] T. Brunner, "Cybersecurity in beyond 5g: use cases, current approaches, trends, and challenges," *Communication Systems XIV*, p. 28, 2021.

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

[41] 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.

[42] M. W. Lucas, *TLS Mastery: Beastie Edition*. Tilted Windmill Press, 2021.

[43] 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.

[44] F. Skopik, *Collaborative cyber threat intelligence: detecting and responding to advanced cyber attacks at the national level*. CRC Press, 2017.

[45] A. S. Coronado, "It auditing: Using controls to protect information assets , by chris davis, mike schiller, and kevin wheeler," 2014.

[46] 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.

[47] J. Meese, "Edited by ramon lobato," 2016, printer: Print on Demand.

A1 Appendix

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

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

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

A1.1 Appendix numbering

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

Temporary page!

LaTeX was unable to guess the total number of pages correctly. As there was some unprocessed data that should have been added to the final page this extra page has been added to receive it.

If you rerun the document (without altering it) this surplus page will go away, because LaTeX now knows how many pages to expect for this document.