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

March 15, 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

1 Introduction

1.1 Brief Context for the Problem

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

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 and national security. Abuse techniques are numerous and constantly changing; they include confusable domains, which is the practice of creating malicious domains that imitate real ones, Phishing, etc.?. 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 important 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, registers , researchers, and law enforcement, in addition to technology solutions ?.

1.2 Motivation

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

tactics.

Not only have significant cases of DNS abuse endangered 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. ?, 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 ? 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 ?. These difficulties are compounded by the average user's short attention span and diminished ability to comprehend information, as demonstrated by cognitive psychology studies like Medvedskaya's ? investigation of adult Internet users' attention spans. According to this research, consuming digital media may have a detrimental effect on one's capacity for sustained concentration, which would make grasping complicated topics even more difficult.

Furthermore, there are ethical and legal consequences to DNS abuse and how to mitigate it in addition to the technical ones. The goal of this project is to close this gap by investigating ways to improve the transparency of DNS abuse mitigation. This study aims to shine light on the present efforts and highlight the obstacles to greater transparency by assessing the current landscape of transparency reports and practices among DNS infrastructure providers. The ultimate objective is to provide a contribution to a system that promotes and enables more efficient and approachable transparency in 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 utilising to mitigate DNS abuse, and how do the transparency reports available from these entities characterise and reflect their efforts? Furthermore,how could these practices and reports inform the development of best-practices for transparency in handling DNS abuse complaints?". This question seeks to uncover the mechanisms, policies, and practices in place to mitigate DNS

abuse and to what extent these efforts are transparent to the public and stakeholders.

1.3.2 Project Objectives

Assess Handling of Abuse Complaints :

- Investigate the procedures and policies that DNS infrastructure providers have in place to handle abuse complaints.
- Document the types of DNS abuses 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, confusable domains, etc 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. 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 a collection of recommendations and considerations for future study and policy creation in this area of internet governance, in addition to offering a comprehensive understanding of the current state of DNS abuse transparency.

1.6 Outline of the report

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 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. 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 required, not only by providing information but also by laying the groundwork for its presentation as a better and essential progression in the battle against DNS abuse.

2.2 Understanding DNS and Its Vulnerabilities

The Domain Name System (DNS) is a significant 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 that highlights the fundamental importance of DNS while illuminating the weaknesses that malicious actors may take advantage of ?.

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 security measures. In addition, privacy-enhancing technologies are being used to encrypt DNS queries, preventing eavesdropping and manipulation, such as DNS over HTTPS (DoH) and DNS over TLS (DoT). The environment of DNS threats and defences is always changing in sync with the Internet. For systems to be robust and resilient, it is essential to understand these weaknesses and the continuous efforts being made to mitigate them. 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.

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 mission to make the online environment more secure. Efforts by the institute, such as Compass Dashboards, provide vital data to registries and registrars that will enable proper decisions on combating DNS abuse. They show the commitment to transparency and education by issuing publications such as the "DNSAI 2022 Annual Report" or "DNSAI Bulletin 2023 04; Account Takeovers," which provide information on DNS abuse and how recommended mitigation practices ?. Another such global strategy against DNS abuse has been contributed by the Internet Corporation for Assigned Names and Numbers (ICANN)?. In collaboration with the entire DNS community, ICANN supports a synchronised method in the development of policies and standards on how to mitigate DNS abuse while ensuring the openness and operability of the Internet. These participatory pillars hint at concerted efforts through policy development, technological developments, and stakeholder engagement as a central component in this collective approach to combating DNS abuse ?.

2.4 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.

2.4.1 Phishing

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

2.4.2 Confusable Domains (Typosquatting)

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

2.4.3 Domain Hijacking

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

2.4.4 Botnets

- **Description:** Botnets involve controlling a group of computers infected with malware, used to carry out attacks or spread spam and malware ?.

- **Mechanism:** Malware infects 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.

2.4.5 Fast Flux Hosting

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

2.4.6 Domain Generation Algorithms (DGA)

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

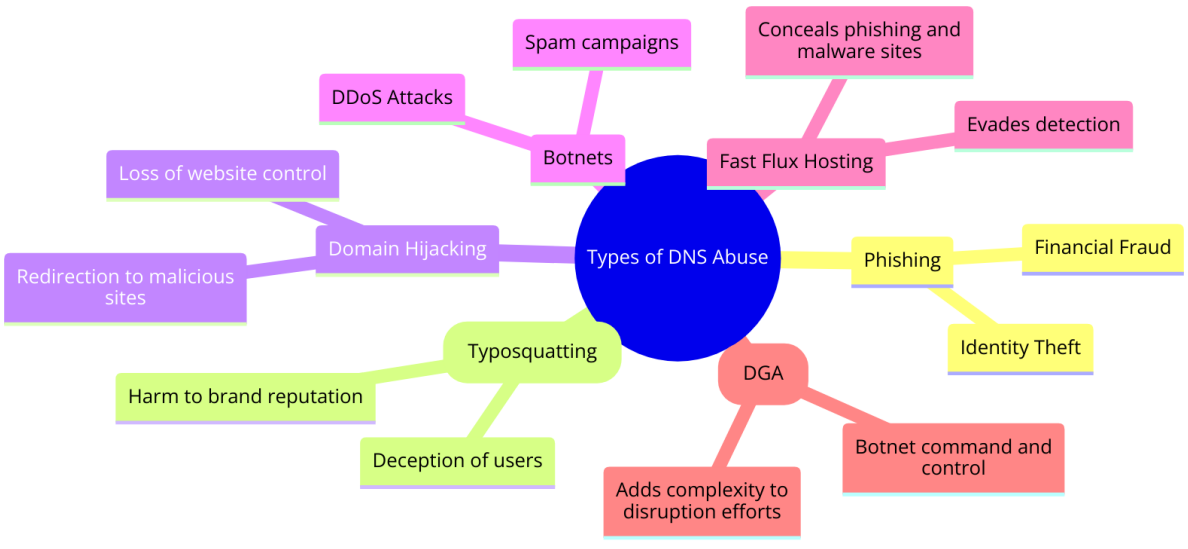

Figure 2.1: Impact of DNS Abuse

2.5 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.

2.5.1 Identity Theft

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

2.5.2 Financial Loss

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

2.5.3 Data Breach

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

2.5.4 System Compromise

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

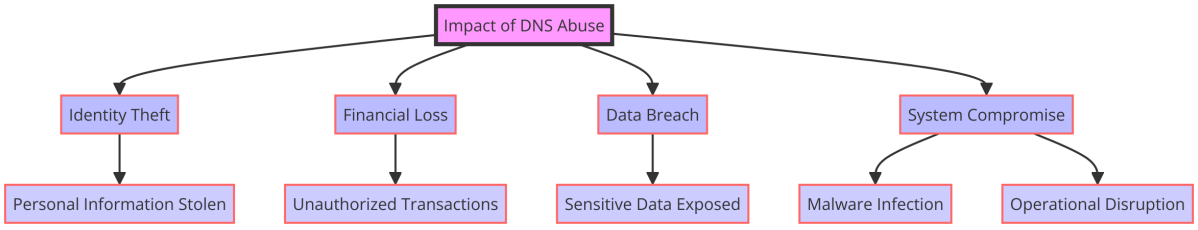

Figure 2.2: Different Forms of DNS Abuse

2.6 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. Bad actors are always creating increasingly

sophisticated methods to take advantage of DNS, such as creating more convincing phishing schemes and using advanced virus distribution networks.

2.6.1 Increased Sophistication

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

2.6.2 IoT Vulnerabilities

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

2.6.3 Infrastructure Attacks

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

2.6.4 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 ??.

2.6.5 Cloud Computing Vulnerabilities

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

2.6.6 Mobile Device Exploitation

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

2.6.7 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 ?.

2.6.8 Political and Information Warfare

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

2.6.9 Exploiting Emerging Technologies

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

2.6.10 Supply Chain Attacks

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

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.

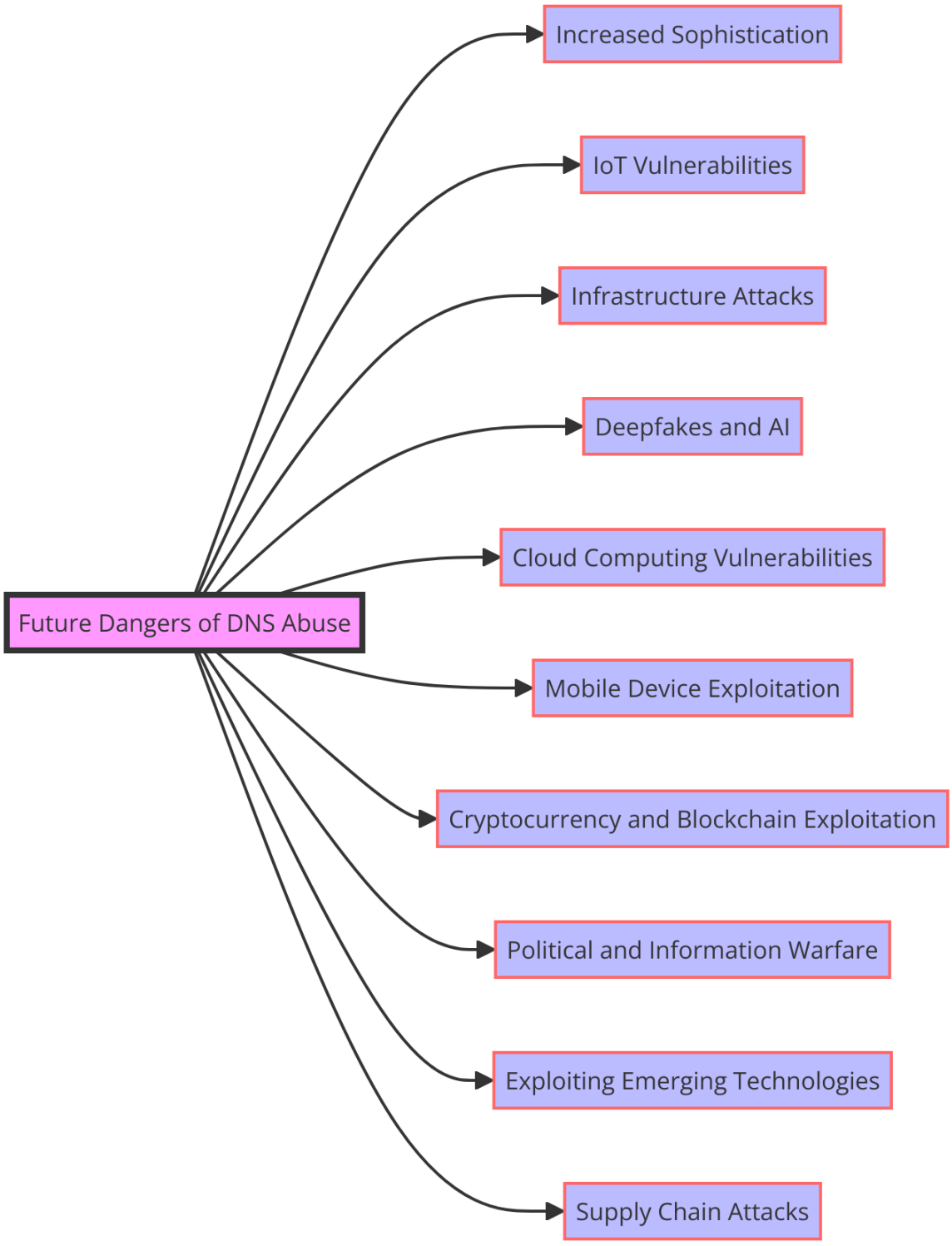

Figure 2.3: Future dangers of DNS abuse

2.7 Foundational Mitigation Strategies and Best Practices

To address the broad nature of the threats, mitigating 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 ?. To confirm security and ensure that systems have not been compromised, regular audits of DNS setups and domain registrations are also necessary ? .

1. **Monitoring and Reporting**
    - Implementation: Use automated systems to monitor the registration of domain names for patterns that may indicate DNS abuse ?. Establish procedures for reporting activities to authorities or cybersecurity organisations ?.
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 ?. This adds a layer of security beyond passwords, helping to prevent unauthorised domain transfers or alterations ?.
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

?.

7. **Regular Audits**
    - Implementation: Conduct security audits of domain registrations and DNS configurations to verify their security and ensure they have not been compromised ?.
8. **Machine Learning**
    - Implementation: Using AI and machine learning algorithms to analyse patterns in DNS traffic and proactively predict instances of DNS abuse ?. This proactive approach enables the identification of threats before they materialise ?.
9. **Geo-Blocking 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 ?.
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 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.

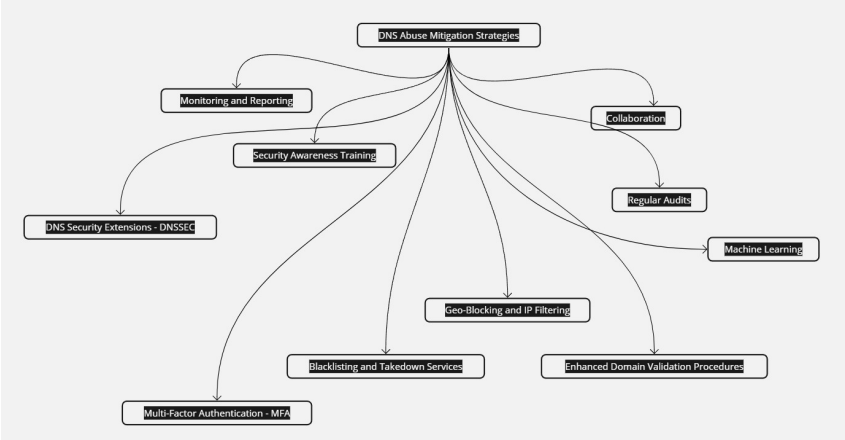

Figure 2.4: Future dangers of DNS abuse

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

Continued on next page

DNS Abuse	User Harm	Mitigation Strategy	Reasoning	Transparency Aspect
Cloud Computing Vulnerabilities	Data Breach, Unauthorised Access	Regular Audits, Enhanced Validation	Secure DNS settings in cloud services. Prevents exploitation.	Framework for secure domain use in cloud.
Mobile Device Exploitation	Unauthorised Access, Financial Loss	MFA, Security Awareness Training	Secures account access. Raises awareness of threats.	Mobile security awareness and protection.
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 mitigate DNS abuse. After analysing the data, it

is evident that a team effort is needed to comprehend, track, and mitigate DNS abuse. A complex strategy that integrates multiple techniques and encourages collaboration across industries is required instead of a single, insufficient strategy. Our approaches to preserving the integrity and security of the DNS and, consequently, the larger internet infrastructure must adapt, as does the digital environment.

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

3 State of the Art

This chapter explores the strategies used to mitigate DNS abuse and new developments in this field. Explore and evaluate the effectiveness and transparency of multiple mitigation techniques, including DNS filtering and threat intelligence in which information about cyber attacks is organised and analysed by experts. 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 face operational challenges, such as errors and the need for fast access to critical threat data.

3.1.1 Transparency in DNS Abuse Mitigation and DNS Relevance

1. A Case Study of Cloudflare's Transparency Approach

   Cloudflare is firmly committed to transparency ?, the cornerstone of its relationship with customers, which guides its approach to DNS abuse reports and requests that

may come from law enforcement. This shaves their actions and policies to mold a trustworthy environment while addressing internet safety and privacy concerns. Their approach to handling DNS abuse reports and law enforcement requests is grounded in three core principles:

(a) Require Due Process: Whatever shall be lawfully requiring due process of law enforcement and Cloudflare shall adhere in letter and spirit. They are neutral in behaviour and do not intend to hinder or facilitate law enforcement efforts more than is required by law.

(b) Respect privacy: At Cloudflare, privacy is very important. They assure customers that anything of personal nature shared by them remains private and protected. The company makes a commitment not to sell, rent or disclose personal information without specific and unambiguous consent from the individual, applying this policy to commercial and government or law enforcement requests.

(c) Provide Notice: Per the CloudFlare policy, they undertake to provide notice to any of their customers in case a subpoena or other legal process issues for customer or billing information relating to the use of its network, unless otherwise such disclosure is otherwise not permitted by law. This is aimed at making sure that individuals and organisations are made aware before theirs can be distributed.

The Cloudflare Transparency Report for the latter half of 2022 gives deep statistics and trends based on DNS abuse reports over Cloudflare's response. It highlights:

(a) Abuse Reports: Cloudflare avidly responds to various abuse reports, and it has shown an enthusiastic commitment to maintaining a clean and lawful network. Some types of abuse reported include phishing, malware, and content that violates copyright laws, among others.

(b) Actions Taken: Cloudflare not only reserves the right to review, accept or decline clients, but also ensures decisive actions against reported abuses by terminating hosting services from the domains taking part in technical abuses, such as phishing or any malicious activities. Such terminations are not limited to actions taken by content-based abuse and are handled differently.

(c) Termination of services: Cloudflare suspends services to domains that do not take action to remedy reported instances of CSAM (Child Sexual Abuse Material) or are otherwise dedicated to distributing such material. Last year, in just the second half of 2022, alone, Cloudflare suspended service for 206 accounts and 530 domains connected to CSAM.

(d) IPFS and Ethereum Gateways: If a valid abuse report is received in regard to

copyright, technical sanctions compliance, or otherwise, Cloudflare reserves the ability to disable access through its operated gateways to content on IPFS and the Ethereum network. 99 actions were taken on Ethereum gateways and 1142 for IPFS during the second half of 2022.

(e) UDRP Requests: 21 UDRP (Uniform Domain-Name Dispute-Resolution Policy) responses resulted from verification requests to Cloudflare by an ICANN-approved dispute board in the second half of 2022, further illustrating its commitment to response in such legitimate concerns regarding domain name disputes.

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

(a) Legal Sufficiency Review: Each request is reviewed by Cloudflare for legal sufficiency before processing. This may range from ensuring compliance with necessary processes to all that is practically feasible within the purview of law to meet the need. They respect and safeguard the privacy of users and provide customer information to written requests from law enforcement that are validly issued based upon laws with valid legal process such as a subpoena or court order.

(b) Respect to International Privacy Laws: Cloudflare recognises the potential conflict of privacy laws of different countries, and when they receive requests from government, they legally challenge any request for data that is conflicting with the privacy laws of the country where the user stays.

(c) Emergency Disclosure Requests : Cloudflare takes very seriously all emergency disclosure requests. They may therefore make such disclosures to law enforcement without legal process when there appears to be an imminent danger of death or serious physical injury, and requests that law enforcement obtain legal process when time permits, therefore ensuring that the use of emergency disclosures remains a carefully controlled exception.

(d) National Security Requests and Non-Disclosure Obligations: Cloudflare has made a lot of effort to challenge FISA court orders or National Security Letters (NSLs) in case they feel that the company received one with which their desire for transparency or releasing transparency reports cannot be met. In this regard, there was a period when the company fought legal prohibitions to report the receipt of NSLs, indicating its attitude of fighting for transparency and user privacy.

(e) International Requests for Data: In the case of requests emanating from governments outside the United States, Cloudflare again evaluates them with

strict adherence. The company responds to requests issued through U.S. courts by way of diplomatic processes like mutual legal assistance treaties (MLATs) and evaluates other international requests on a case-by-case basis. These include an analysis of local law, the request's compliance with international norms, and company policy.

(f) Challenging Overly Broad or Inappropriate Requests: Over time, Cloudflare has long stated that it will challenge any law enforcement requests that are overbroad or issued wrongly and that act as an obstacle to their transparency with users. ., provided that due process of law requirements are met or that the exercise is intended to protect user rights in any request they may receive in or outside the USA.

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

(a) Reporting to the Public and Transparency: Cloudflare keeps a high level of transparency in its reporting with regard to the types and volumes of abuse reports it receives and the measures which are put in place. This supports the creation of trust among clients and partners, demonstrating action in the fight against abuse.

(b) Law Enforcement Cooperation: The report shows how Cloudflare interacts and cooperates with many law enforcement agencies in the most approachable manner and without touching upon user privacy. It enables careful consideration of such a request for any action to be legally justified and, by so doing, contributes to general mitigation efforts of DNS abuse.

(c) Mitigation Actions: Cloudflare has taken affirmative action against DNS abuse. These actions include, but are not limited to, terminating such services when knowing of domains being used for phishing, distributing malware, and performing other activities that would harm a greater world. Termination of the access is done on content at the many different access points provided by Cloudflare, including any relating to abuse reports and, indeed, including IPFS and Ethereum gateways. This shows that the company is serious about mitigating DNS abuse.

(d) Challenges to Preventing DNS Abuse: While Cloudflare does provide these tools, the report still refers to challenges that come with abuse mitigation. The struggle for balance between protection and abuse of free expression, legal and technical challenges when reacting to abuse reports, and from what kind of cooperation between key shareholders are, it is underlined, ongoing challenges.

(e) Efficiency of Efforts to Mitigate DNS Abuse: Cloudflare transparency practices, through the half-yearly publication of transparency reports, lend a hand in acquiring insights into the mitigation of DNS abuse. This clearly shows their commitment and forward-leaning policy to minimise problems related to DNS abuse. However, its efficacy also depends on the broader ecosystem's capacity to solve the initial cause of this DNS abuse, an undiversified market where most other options for hosting are very limited.

Some of the challenges with which Cloudflare is confronted in its transparency efforts and in mitigating DNS abuse are mentioned in the Transparency Report . They include such matters as the complexity of DNS abuse, keeping the fine balance between transparency and privacy, legal/regulatory compliance, and limitations of technical ability in mitigating the misuse while keeping the fine line. With these insights in mind, the following are recommendations that Cloudflare could use to identify potential enhancements in its processes:

(a) Enhanced Cooperation with Stakeholders: Cloudflare will enhance cooperation with law enforcement, other service providers, and international organizations to exchange views on best practices and come up with standard operational procedures on how exactly they will address DNS abuse. Joint efforts reduce identification time and intensify the ability to mitigate abuse throughout the whole of the internet ecosystem.

(b) Improve Abuse Detection Systems: Continuous investment in the best technologies and machine learning algorithms will improve abuse detection and enhance its ability to respond to DNS abuse. Better detection will be less time-consuming in identifying and bringing down abusive content, therefore improving the entire internet safety concern as a whole.

(c) Transparency Reporting Enhanced: The reports on transparency from Cloudflare are simple to understand, yet they need more details about the identification of types of abuses faced by the domain name system and evaluate the process with respect to checking its effectiveness on all counts for mitigation. It will keep stakeholders up to date by providing much more details when it comes to trend and pattern assessment in regard to abuse, which will lead them in the process to fine-tune the directions of best practices for abuse mitigation.

(d) Better User Education and Awareness: Cloudflare would be in a position to prepare more materials and programmes that educate its users about cybersecurity and the risks of DNS abuse and what they should do for protection. Enhanced user engagement in these can help build an enhanced internet environment.

(e) Advocate Policy and Legal Reforms: Cloudflare can do more to try to advocate for policies that will potentially be challenged at various legal jurisdictions and cause a potential conflict of privacy laws against law enforcement requests. In such a push for already formulated laws and put-in-place policies to balance user privacy against those interests supporting efforts in fighting DNS abuse, an improved offer may be realised. This policy helps offer protection against the abuse or even support for more coherent and efficient internet governance.

(f) Create a Multi-stakeholder Feedback Mechanism: A mechanism can be framed that ensures feedback from users, civil society, and other stakeholders that would indicate how far Cloudflare has been successful in its transparency efforts and reducing abuse. Such suggestions thus received can then guide any subsequent policy revisions or enhancement of organisational policy.

(g) Continue to Challenge Overbroad Requests: Cloudflare's willingness to continue fighting even with overbroad or inappropriate requests for user data in place remains praiseworthy. The possibility of being able to further prioritise the user and due process amongst this sort of situation implies some more badge of trust and a role model for the industry.

To conclude, the company highlights its commitment to upholding legal processes and user privacy while navigating government and law enforcement requests. A critical aspect of these reports is Cloudflare's approach to DNS requests, particularly regarding content blocking through its 1.1.1.1 Public DNS Resolver.This was the key answer: Cloudflare, in no uncertain terms, "received legal requests to block content at our DNS servers" and stated its policy to first "exhaust legal remedies" that they could enforce. This is an indication of how very carefully Cloudflare has to adhere to the demands of the law yet protect the openness of the internet, bringing out just how major DNS is in all matters that pertain to the accessibility of content on the internet and governance of the internet.

2. Google Transparency Reports

it has become evident that there lies a relationship more dynamic in nature between the governments of the world and internet governance, specifically through requests for removal of contents in the Google services. In light of this, the function of the Domain Name System comes up as one of the mechanisms that are critical in realizing how the requests can be translated into actions. The relevant data, e.g., for Russia, contains tens of thousands of items to be redacted. Massive redaction requests, such example, go very far beyond the issue of focused content take-down and indicate potential for the far broader action up to and perhaps including that which would be taken on the DNS level and through other means that may be ultimately settled here

on the domains to be held in enforcement. Such instances further highlight all the more the role of DNS in enabling access to or blocking content on the Internet while serving much more effectively as the gateways through which governments indeed wish to exercise control, for which legal and regulatory pressure is employed so often on large technology companies like Google.

Further, the queries clarify the relevance of DNS; they do not directly mention "DNS manipulation" but phrasing points to some kind of 'how-to' on technical compliance, which could also be the making of DNS changes. The compliant removal requests that are yielded to by Google indicate technical mechanisms that may be in place to comply with government mandates and are most likely affecting how DNS resolves to certain domains or URLs. This indirectly points to the DNS as critical infrastructure within the larger debate on Internet governance, censorship, and access to information. Seen in the light of that Google Transparency Report, it becomes very telling that DNS clearly breaks through this legal and policy structure not only as an underpinning element to the architecture of the Internet but as a very hotly contested space to control both digital content and information flow ?.

3. Amazon Transparency Reports

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

4. DNS- SB Transparency Reports

   xTom reported nil compliances, for the most part, within the international statistics of content data requests, requests for information on subscribers, requests to have content taken down, requests to have content blocked, and domain name dispute resolutions in 2020. These zero compliances are placed to highlight the fact that the organization, in reality, set the protection level of user data and content integrity too high in which a part of a general position on how DNS and domains are managed for protection of users and reaching operable thresholds ?.

5. The CyberGhost Transparency Report

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

6. The Meta Transparency Reports

   This will also touch on enforcement of intellectual property on social media platforms like Facebook and Instagram, and usher overall holistic measures to fight violations on copyright, counterfeit, and trademarks. The DNS is important to these functions along these two aspects. First, with regard to it being an underpinning of the distribution of information online and, on another sense, a checkpoint in the process of enforcement. For instance, Facebook removed 447,123 pieces of content on copyright grounds, and on Instagram, 297,356 in the first half of 2022. Taken in such high volumes, one would easily conclude that beyond the platform level of moderating content, other interventions at the DNS level had to be made. Those could vary from steps like de-indexing websites from search, to editing DNS records, in such a manner that requests to domain names of abusive sites are not resolved or that access to infringing content is denied.

   Results since the second halves of 2020 and 2021 seem to suggest that the rates of removals have been self-sustaining, due to the mechanisms of DNS dependency. Last year, in 2020, Facebook stuff removed 432,854 pieces of content for copyright reasons, but this number decreased to 273,325 counterfeit items removed in 2021. This is a huge amount, proving that if something was taken down, then Meta has not only removed nasty content from offers but most likely reached an agreement with DNS providers too, to not allow access to offending domains. This clearly elaborates on the integral part of the DNS in enforcement, hence they are used in upholding intellectual property rights, effectively lessening the spread of counterfeit goods, and protecting the interests of creators and owners of the trademarks ?.

3.1.2 Advanced Mitigation Strategies

Different methods are used to mitigate DNS abuse, including the implementation of blocking tools, awareness of potential threats, and identification of anomalous behaviour. DNS filtering entails the regulation of website access based on predetermined rules, which can have varied outcomes depending on the context in which 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 block-lists and predefined rule to identify potentially malicious homographs as stated earlier. Threat intelligence plays a role in identifying potential dangers and detecting unusual activities within the DNS, as noted ?, such as allowing the proactive identification and assessment of potential threats and malicious activities, including detecting patterns indicative of phishing, domain hijacking, malware distribution, and other forms of DNS abuse. Evaluating the effectiveness of these methods requires careful consideration of their performance in real-world scenarios. For 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 utilised. However, identifying anomalous behaviour poses challenges, as distinguishing between malicious actions and legitimate activities performed in innovative ways can be challenging.

3.2 Emerging Trends in DNS Abuse

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 behaviours. One such move to enhance user privacy is the Query Name Minimisation. The main concern has been how to remain vigilant against DNS abuses while improving privacy without 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 emphasise the proactive and reactive measures but also the possibilities of increased transparency as far as reporting and publicising the actions in place against DNS abuse are concerned. Such transparency is key to building trust, open 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 interpret-ability is a significant challenge. Therefore, it is essential to approach this challenge with caution, ensuring that the models are not only effective in identifying DNS abuse, but also accessible for thorough examination and accountability.

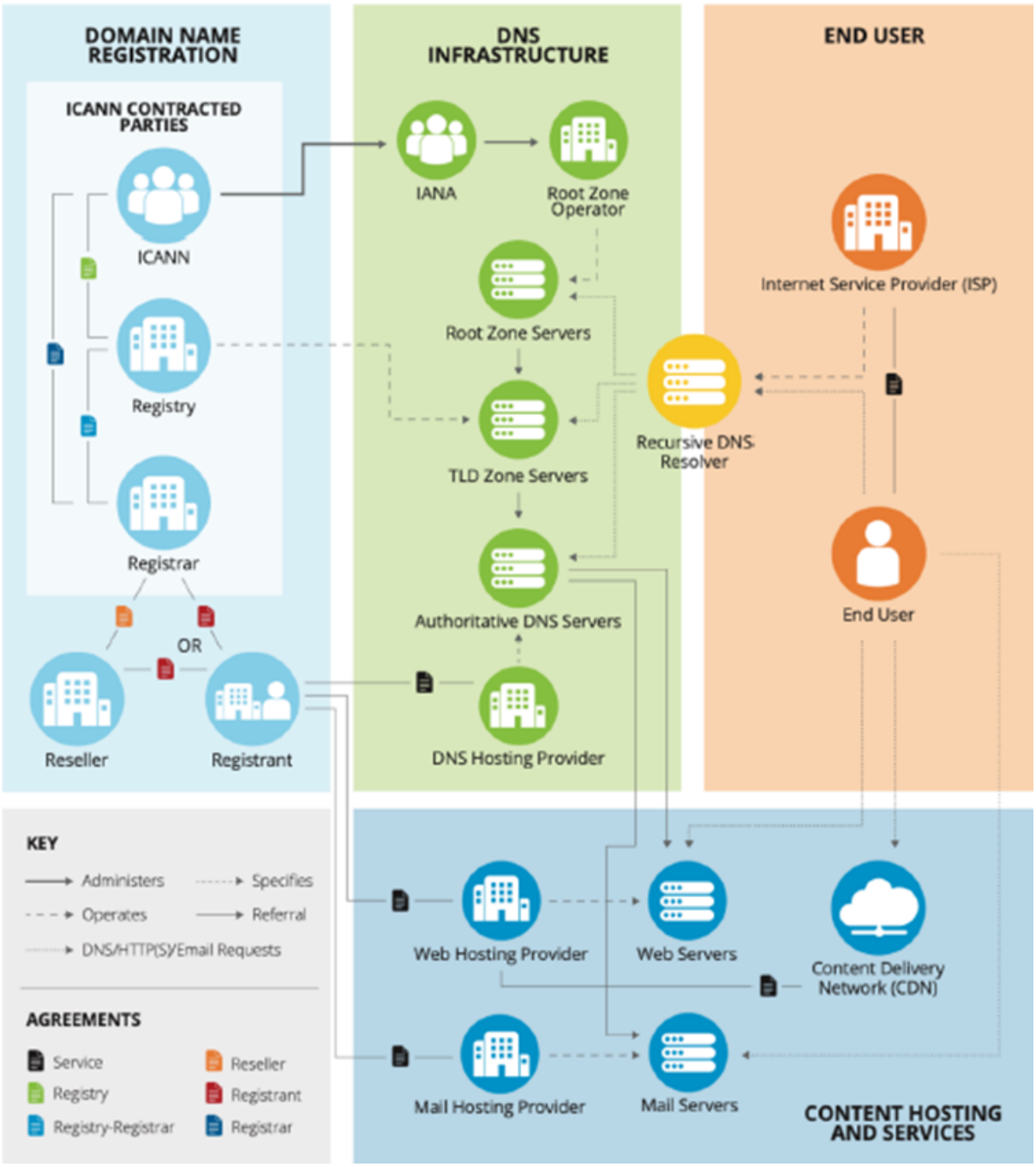

Figure 3.1: DNS Ecosystem Contractually Related to ICANN (image courtesy of Verisign and originally published in SSAC 115)

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 neutralisation of cyber threats ?. This approach facilitates the rapid analysis of large datasets to uncover patterns indicative of malicious intent in DNS queries. For example, machine learning techniques have been highly effective in analysing DNS queries to classify domain names, significantly improving the detection of domains linked to malware ?. Furthermore, the application of neural network models, such as the Extreme Learning Machine (ELM), has achieved accuracy rates above 95% in 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 ?. 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.

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.

3.4 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.

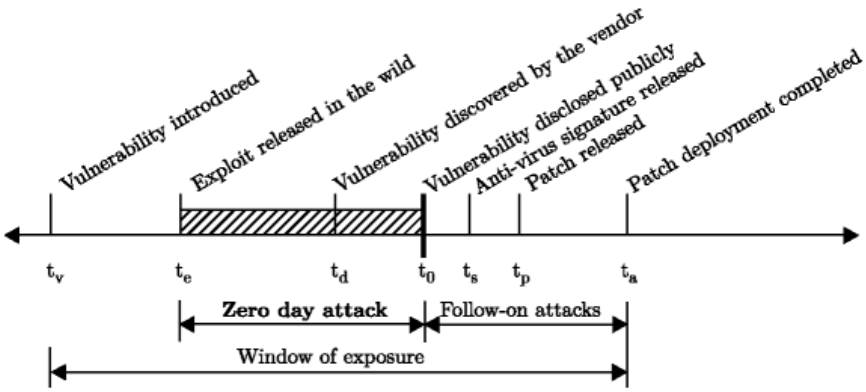

Figure 3.2: Timeline of DNS Abuse Attacks on XYZ Corporation

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 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.

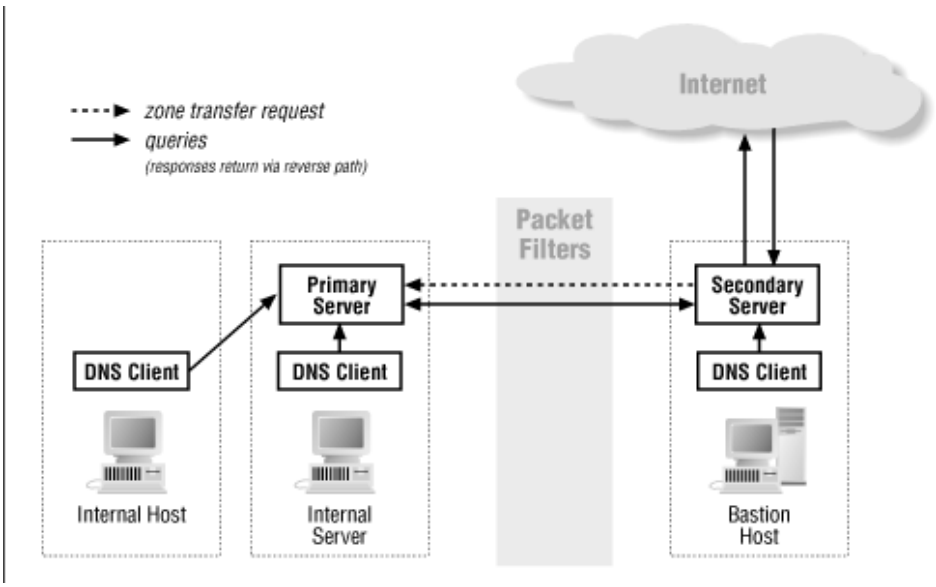

Figure 3.3: Distribution of DNS Abuse Techniques Against XYZ Corporation

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 multi-factor 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 ?.

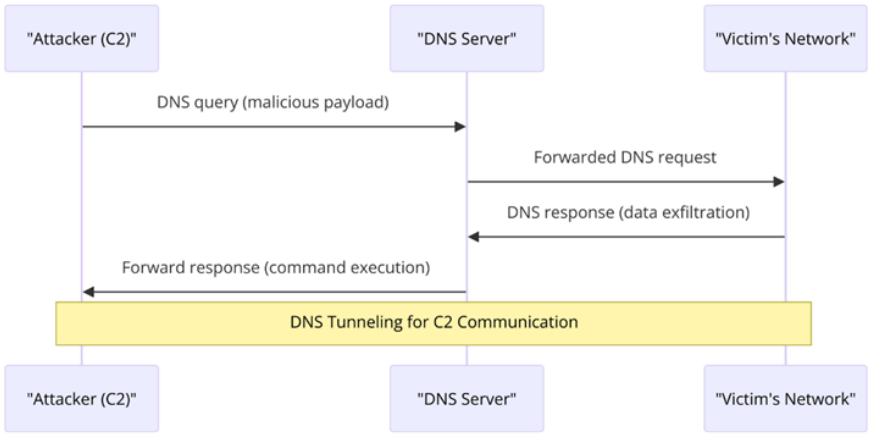

Figure 3.4: DNS tunneling communication between the attacker's command and control (C2) infrastructure and the victim's network

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 ?.

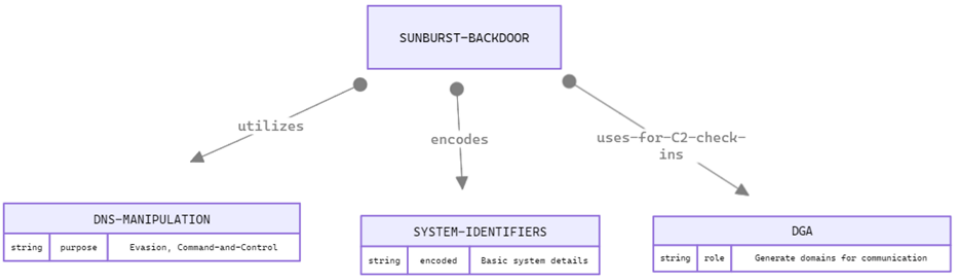

Figure 3.5: SUNBURST backdoor's utilization of DGAs and its associated components

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 ? .

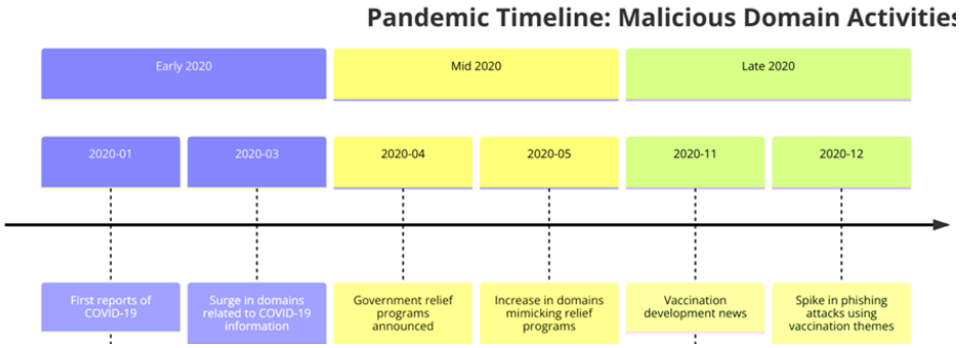

Figure 3.7: The usage of Fast Flux techniques by the Smoke Loader malware family for dynamic C2 domain communications.

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 US 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 organisations 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 have been received, 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%. The results showed much steadier phishing when it came to topics such as pharmaceuticals and virtual meeting platforms (e.g., Zoom) with vaccines and testing showing sharper rises and falls in the attention of scammers.

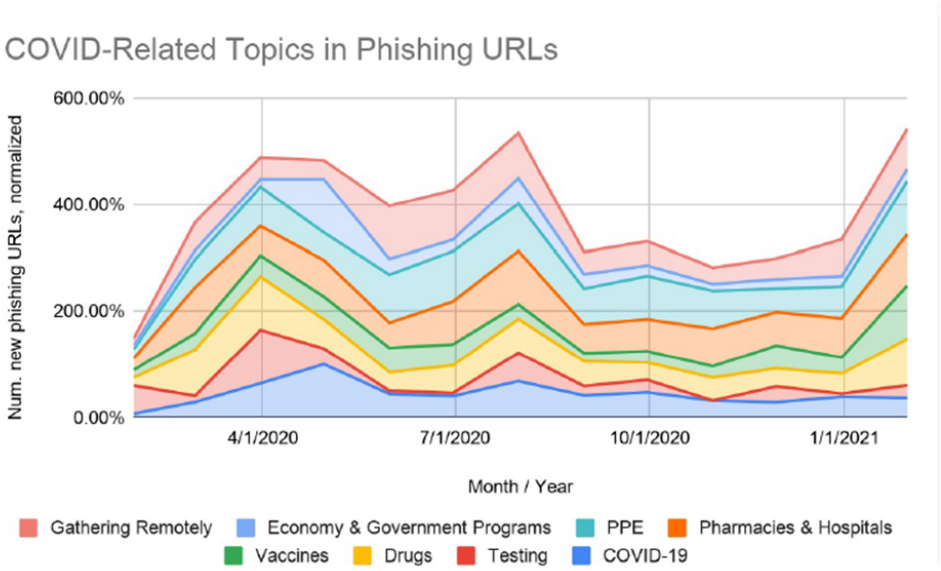

Figure 3.8: Development trends in the majority of COVID-19-related phishing content hosting sites during the period from January 2020 to February 2021.

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 were posed as Microsoft login pages. This threat has particularly highlighted the shift towards remote work in the pandemic and, hence, magnified the relevancy of these attacks as one of the foremost methods to be undertaken by cybercriminals.

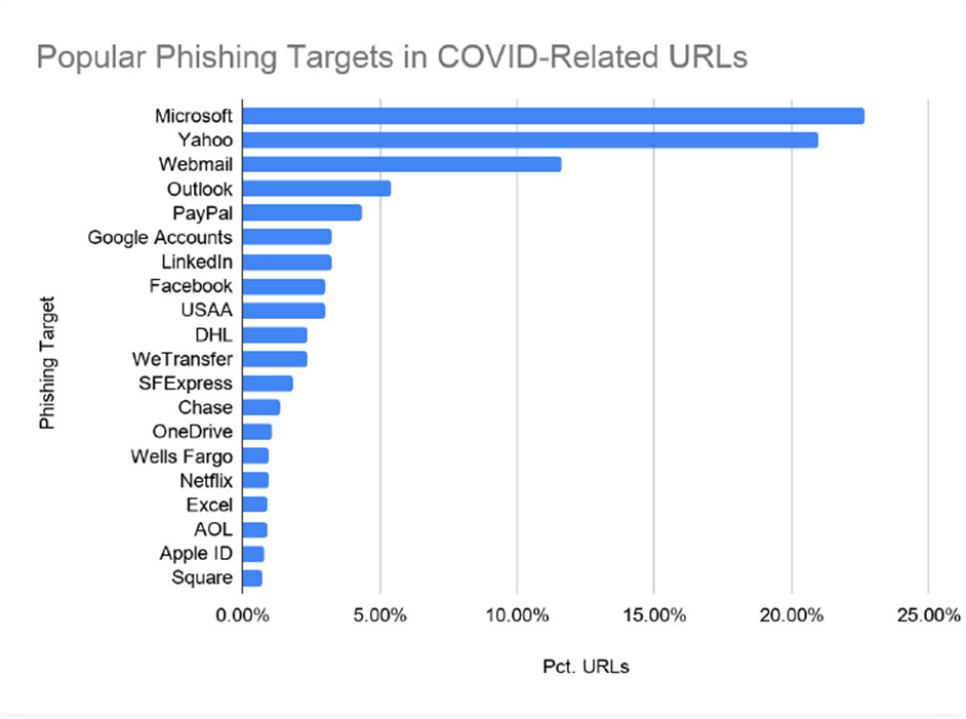

Figure 3.9: Top spoofed websites in COVID-themed phishing attacks (global), where the percentage in each column is the percentage of phishing volume per site and category.

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

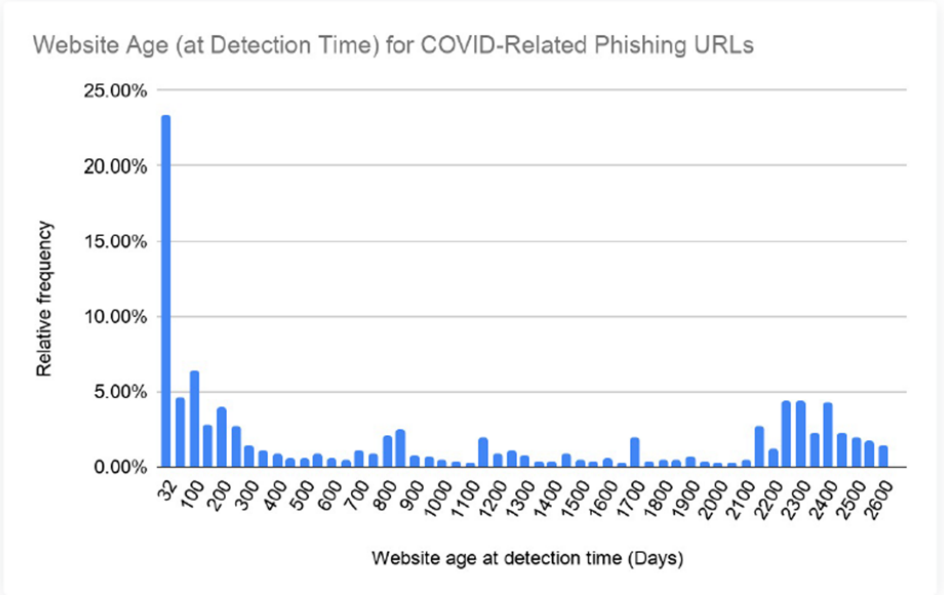

Figure 3.10: Statistic of lifespan distribution of COVID-19-related phishing content hosting sites when the sites are reported .

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 important. 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, which 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 in which DNS operates on a network of distributed nodes in which each node has a copy of the entire 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.

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 new 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 Research

4.1 Introduction to Research Methods

A structured questionnaire was sent via email to various stakeholders in the DNS ecosystem. This method was chosen because of its convenience, compliance with participants' busy schedules, and permission for detailed responses at the respondents' will. The approach provided a means of soliciting a wide range of expert observations on DNS abuse in terms of definition, the most prevalent types, mitigation challenges, and the theme of transparency. Emailing was chosen to reach the various players so that a much greater participation level would be reached, suitable to the schedules of the large number of participants, yet permitting ample space for an in-depth approach to the subject. Such an approach has made it achievable to strike a balance for both accessibility and convenience for participants while meeting the need for comprehensive data collection.

4.2 Questionnaire Design and Distribution

The questionnaire had to take into account all of these issues in a multidimensional approach, giving great emphasis, but not limited, to the following definitions, types encountered in practice, challenges of dealing with mitigation, and considerations regarding transparency. Even at the very outset, the respondent could be invited to agree or state their view of a well-known definition of DNS abuse, thus showing this matter to be diverse in application and interpretation.

The questions were carefully crafted to elicit detailed insights on:

1. the definition of DNS abuse.
2. The types of DNS abuse stakeholders most commonly encounter, aiming to identify prevalent patterns and specific concerns within the ecosystem.
3. The challenges and limitations faced in mitigating DNS abuse, seeking to understand the barriers to effective action.

4. The mitigation strategies employed, gathering information on the practical steps taken and their perceived effectiveness.
5. The practice of publishing reports or data as a form of transparency, exploring the current state of openness in the field.
6. The role of transparency in aiding or impeding DNS abuse mitigation efforts, probing the potential impacts of increased visibility.
7. The effects of transparency on the relationships between various DNS stakeholders, considering the broader implications for cooperation and trust.

These participants are key stakeholders who are directly involved or have experience in the DNS ecosystem, such as operators, registrars, registrants, and regulators. This selection presents comprehensive points of view that could allow for varied views for the study.

4.3 Stakeholder Responses

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

Key Themes and Insights:

- **Varied Definitions of DNS Abuse:** Although stakeholders largely accepted the definition that had been adopted by the ICANN Contract Parties, they also noted its shortcomings, especially in being too categorical, and thus may leave out evolving types of abuse. It was considered that a more flexible way forward would be a robust framework for defining the abuses to be mitigated at the domain name level.
- **Common Types of DNS Abuse:** They pointed out that phishing was the most common attack type, followed by malware, botnets, and spam. It was also pointed out that one of the most common problems was linked to the challenge related to proving the quantity of spam-related domains.
- **Challenges in Mitigation:** Perhaps the most significant was the economic structure of the domain registration industry, its ability to mitigate malicious registrations without fundamentally altering it. The stakeholders clearly state that a significant difference between large registrars, generally considered good actors of the internet,

and smaller registrars with a higher level of DNS abuse underscores the different aspects of this problem within different industry segments.

- **Mitigation Strategies:** The responses included different strategies, such as blocking orders from some regions or using software to monitor abusive activities. Recommendations were made regarding the role of education and outreach, including relevant projects such as NetBeacon and Compass for abuse reporting and insights for DNS abuse.
- **Role of Transparency:** Opinions on transparency were mixed since part of the respondents consider this positively as it is a tool that provides evidence to the industry in its fight against abuse, part of them considers it negatively as sensitive mitigation ways could be revealed. The impact of transparency was also elaborated on developments in relationships between all stakeholders, and there is in general agreement that transparency will increase understanding and teamwork through better communication on measures set against abuse.

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

4.4 Types of DNS Abuse Encountered

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

- Phishing

Generally, phishing was identified by stakeholders as the most prevalent form of DNS abuse and the most visible. Indeed, the overall number of phishing incidents observed through tools like NetBeacon and tracked by Compass is a stark and singular metric for just how big and urgent the problem has become across the wider DNS domain.

- Malware and Botnets

Those also included malware and botnets, that is, multifaceted DNS abuses. Such abuses compromise not only the integrity of systems but also present a security hazard to users and infrastructures in general.

- Spam

Spam is now recognised as widespread, and stakeholders have pointed out the challenges of quantifying and appropriately addressing the relevant spam-related domains. Therefore, it makes spam elusive for existing mitigation efforts that raise the bar with respect to the pursuit of next-generation detection and response mechanisms.

- Compromised CMS

Compromised content management systems (CMS) have been referred to as a common encounter. Consequently, such attacks are possible in cases of some other existing vulnerabilities in web platforms. This kind of abuse reinforces the need for strong web security control practices and the need for vigilance among platform operators.

- "Water Torture" Attacks

"Water torture" attacks, or random subdomain attacks, represent a more technical and sophisticated form of DNS abuse. These attacks not only disrupt normal DNS operations but also require advanced countermeasures to effectively mitigate their impact.

The varied nature of DNS abuse that stakeholders encounter underlines the fact that community efforts must continue building on ongoing collaboration, innovation, and education to address these challenges effectively. This is drawn from the experiences of stakeholders and forms a basis of paramount importance on which effective strategies and policies will be formulated in the mitigation of DNS abuse.

4.5 Challenges in Mitigation and Mitigation Strategies

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

Economic and Technical Hurdles

A significant barrier identified was the economic structure of the DNS industry, characterised by low margins and high volumes, which often limits the resources available for robust mitigating DNS abuse efforts. Stakeholders highlighted that about 80% of malicious domain registrations could be traced back to a mix of large, well-known registrars and smaller entities with disproportionately high levels of abuse. This economic reality complicates the implementation of effective mitigation strategies, underscoring the need for innovative solutions that are both cost-effective and scalable.

Regulatory Gaps

The regulatory environment was also cited as a challenge, including poor, weak, or absent policies and enforcement mechanisms that could not effectively handle DNS abuse

effectively. Stakeholders pointed out the necessity for clearer regulations and standards that can guide the industry's anti-abuse efforts more effectively.

Mitigation Strategies

Stakeholders have responded to this with a variety of mitigation strategies. They placed an emphasis on components of education, collaboration, and outreach to raise awareness and develop a societal response to DNS abuse. Technological solutions such as abuse reporting intermediaries (NetBeacon) and measurement projects (Compass) that measure the internet are vital in the finding, reporting, and understanding of the abuse cases. Designed to improve reporting and mitigation, these tools can also capture essential data with a character that helps inform policy and regulatory responses.

4.6 Transparency in DNS Abuse Mitigation

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

- Benefits of Transparency :

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

- Challenges and Concerns :

However, at the same time, stakeholders raised several concerns about the degree and manner of transparency. One point of concern is that some sensitive mitigation strategies could be exposed that, in turn, could serve as a support for malicious actors, allowing them to discover ways to detect and mitigate abuse. This fine balance between providing useful insights and protecting operational integrity is a significant challenge for many in the industry. Furthermore, there is apprehension that increased transparency might lead to regulatory or legal repercussions, especially if disclosures are mandated in a manner that

does not consider the practical aspects of abuse mitigation. Stakeholders also mentioned operational challenges, such as the capacity for comprehensive transparency reporting, given the current reliance on less formal mechanisms for abuse reporting and mitigation tracking.

Strategic Approach to Transparency :

Stakeholders advocate for a strategic approach to transparency that supports the goals of DNS abuse mitigation without compromising the effectiveness of these efforts. This includes targeted transparency that focuses on aggregate data and trends rather than detailed disclosures of specific mitigation actions or techniques. Additionally, fostering an environment where sharing information does not lead to punitive outcomes but rather supports collaborative improvement is seen as essential. Although the value in transparency for DNS abuse mitigation is considered high, stakeholders cautiously advocate that every step be done carefully with regard to what, how, and to whom it shall be disclosed.A balanced approach that enhances the collective ability to address DNS abuse while safeguarding the methods employed is crucial for the ongoing evolution of transparency practices in the industry.

4.7 Impact on Relationships within the DNS Ecosystem

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

4.8 Analysis and Data

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

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

Table 4.1: Varied Definitions and Understandings of DNS Abuse

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

Table 4.2: Types of DNS Abuse Encountered

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

Table 4.3: Challenges in Mitigating DNS Abuse

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

Table 4.4: Mitigation Strategies Employed

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

Table 4.5: Transparency in DNS Abuse Mitigation

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

Table 4.6: Impact on Relationships within the DNS Ecosystem

In analysing the data from the stakeholder responses, a thorough examination of DNS abuse has been undertaken. The stakeholders, deeply embedded in the DNS ecosystem, provide valuable insights into the definitions and manifestations of DNS abuse. They highlight phishing as the most frequent and concerning type, with compromised CMS also noted for its prevalence. Challenges in mitigation are predominantly tied to economic factors and regulatory gaps, where the industry's structure impairs anti-abuse actions and a lack of clear regulations muddies the waters. Mitigation strategies like targeted blocking and collaborative education are in play, though their implementation faces hurdles due to the industry's focus on throughput and the capacities of various entities. The role of transparency is acknowledged as double-edged: while it could foster accountability and trust, there is a risk of sensitive techniques being exploited by abusers. The stakeholders' experiences and strategies contribute to a deeper understanding of DNS abuse, suggesting the need for a multifaceted approach that involves adaptation, collaboration, and a careful balance of transparency.

5 Implementation

5.1 Introduction

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

5.2 System Overview

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

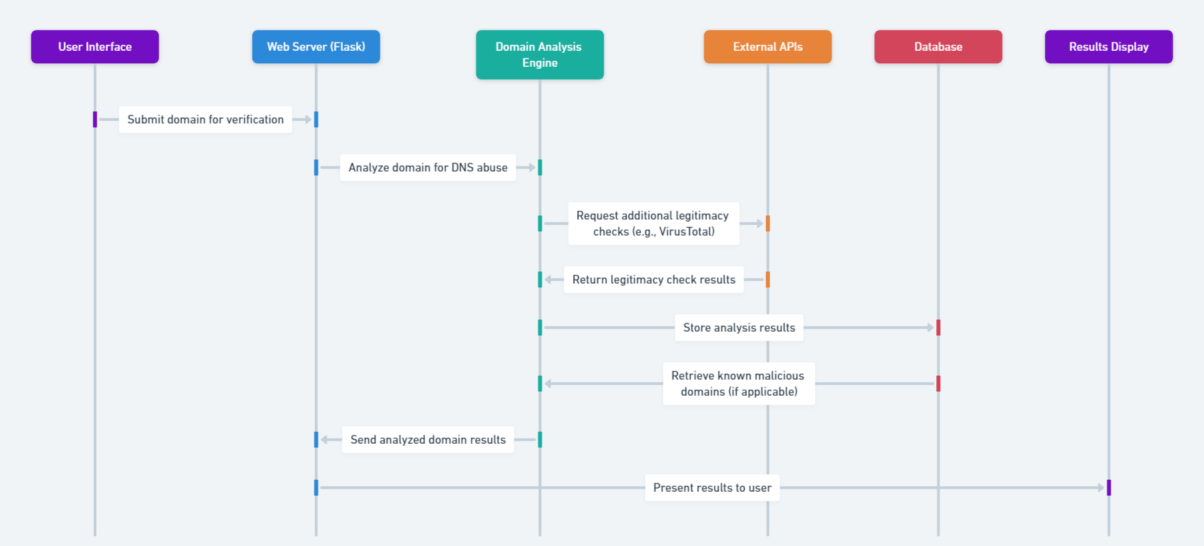

Figure 5.1: Domain Legitimacy Checker

5.3 Integration

5.3.1 Backend Implementation

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

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

Figure 5.2: Domain Legitimacy Checker System Interaction Workflow

5.3.2 Frontend Implementation

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

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

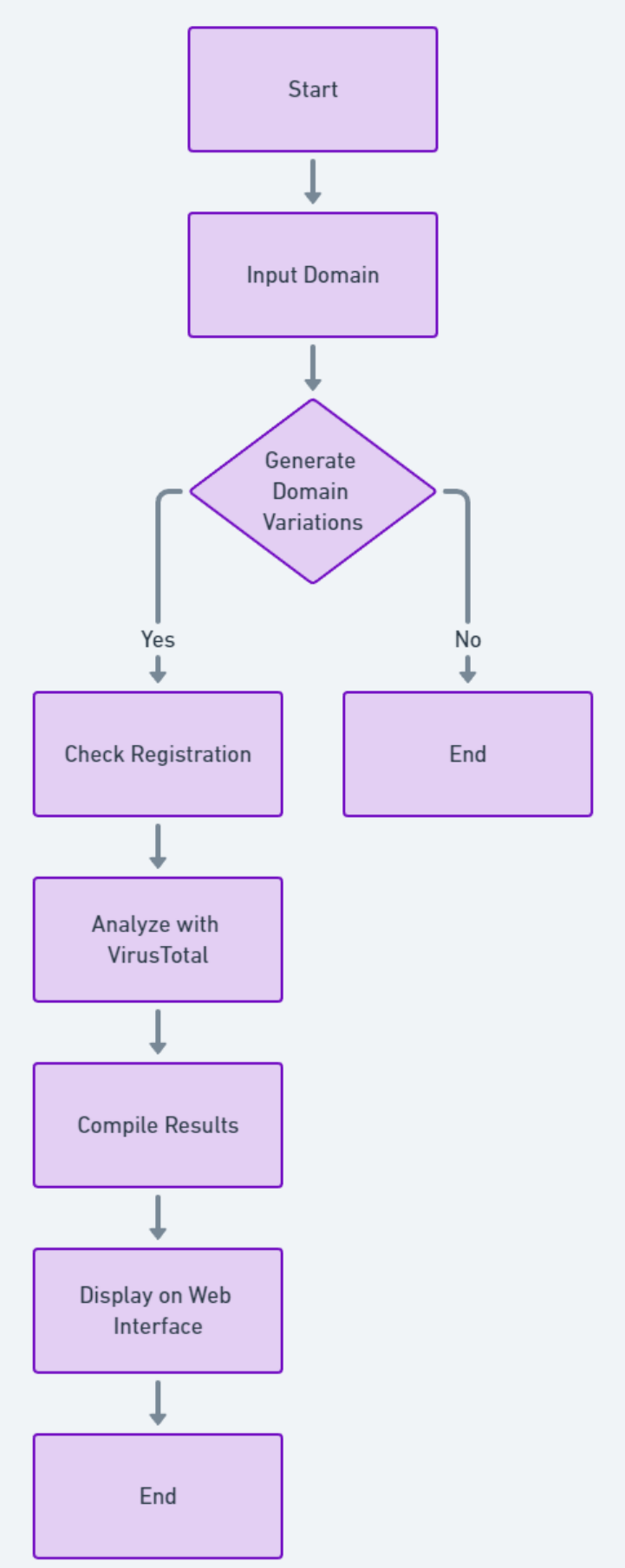

Figure 5.3: Domain Legitimacy Checker

5.4 Tools and Technologies

The Domain Legitimacy Checker was constructed using a carefully selected stack of tools, languages, and platforms. The primary language chosen was Python, valued for its readability, comprehensive standard library, and wide range of third-party modules that facilitate rapid development and integration with other systems. As a result, the decision was made to stick with Flask as an interactive back-end web framework, since in connection with its extremely light character, it's easily scalable and updatable in nature. Though designed very simple, it's versatile enough to really cover all major issues regarding painful threads of HTTP-requests processing.

For the frontend, HTML5 was the markup language of choice for structuring content on the web, while CSS3 was used for styling, ensuring a modern and engaging user interface. Bootstrap, a widely-used frontend framework, was integrated to expedite responsive design, allowing the interface to adapt to various device screens without extensive custom code. It is very important to ensure that a system runs smoothly by making the development of dynamic and interactive web pages using JavaScript. In the system, the scripting at the client side has used plain JavaScript so that it may maintain simplicity and hold onto any control over all the behaviours implicated.

The dnspython library provided the tools necessary for DNS queries, allowing the system to programmatically interact with DNS records, an essential feature for checking domain registration status. To conduct external checks for domain legitimacy, the requests library facilitated communication with external APIs, such as VirusTotal, renowned for its extensive database and reliable threat analysis.

The VirusTotal API was utilised due to its comprehensive scanning capabilities, which leverage a multitude of antivirus engines and website scanners to assess the security of a domain. The scope of its scanning will come from thousands of antivirus engines and websites that will check if the domain is ok to browse or download. Equally important in the DNS Abuse System is the ability to establish the analysis of a wide spectrum of potentially abusive domains. VirusTotal searches for a record of if the supplied domain has ever been blacklisted before for hosting phishing sites, spreading malicious software, or in general, being accessed for carrying out other suspicious actions. Such a dataset is to be found within the very repository of the API, thereby making available unmatched data and accuracy for threat detection, hence by and large enhancing the capability of this system in terms of protection against DNS related cyber threats.

Each tool and technology were chosen not only for its individual merits but also for how well it integrated with the others, ensuring a cohesive and efficient system aligned with the project's objectives of DNS abuse detection and transparency.

5.5 Challenges and Solutions

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

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

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

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

Solution: Using asynchronous JavaScript to send information to the servers and receive results from them without refreshing the web page. The user also receives a form of visual indication in the form of a bar on the point of progress as the analysis unfolds in real time.

Challenge 3: Handling Malicious Domain Variations Identification and generation of a full set of confusing domain variations represented a key computational challenge. Solution: Utilising a combination of common substitution algorithms and a heuristic approach that prioritised variations based on their likelihood of being used in phishing attacks. That way, it helped us match the balance of well-performed search against the practical need for it and against timely results.

Challenge 4: Data Storage and Retrieval Efficiency Storing analysis results for quick retrieval while managing database performance was a concern, especially with the growth of the dataset. Solution: Selecting a suitable relational database management system with efficient search capability in terms of indexing and structured schema that would help provide faster lookup. Regular maintenance routines were established to optimise database performance.

Challenge 5: System Scalability As the system's user base grows, so does the load on our servers, which initially led to concerns about scalability. Solution: The system was architected with scalability in mind, using Flask's built-in capabilities to handle an increasing number of simultaneous user requests. By addressing these challenges with careful planning and adaptive solutions, we enhanced the system's reliability, performance, and user satisfaction.

5.6 Testing and Validation

Domain Legitimacy Checker follows rigorous measures in testing the system, which assures both dependability and accuracy. In the implementation, back-end logic had the number of things implemented with unit tests; we have used the Python unittest framework. We used mock objects for simulating the acts of the external APIs.

Both manual and automated testing were conducted in front-end technologies. Automated UI testings, such as with Selenium, were relied upon to ensure all interactive elements are operable. The interface has been tested both automatically and manually, with the help of loading a page on a few browsers and mobile devices to guarantee the interface is responsive and behaves alike.

I have done practice methodologies of test-driven development (TDD) within overall projects to simulate a lot of real-time scenarios. It will thus ensure the detection of the problem automatically in the early stage, which is necessary for further appropriate rectification. We also set up Continuous Integration (CI) pipelines that would fire every time a new code commit passes to run tests, ensuring newly made changes do not break existing functionalities automatically.

This was done by the system validation against known patterns of DNS abuse, and explanatory notes on the results are attached. Regular peer reviews were also held at regular intervals for the same purpose of reassessment of performance and reliability of the system.

5.7 Conclusion

The implementation of the DNS Abuse Transparency Reporting system reflects a significant stride towards addressing the complexities of domain name security. The chapter presented how integration of these different technologies finally translated into implementation of the platform on the ground for DNS abuse detection, which had reliable results. Key learnings included at what point the right tools should be chosen when it came to scaling and how testings done in an iterative way make the different functionalities stronger. Future enhancements could focus on incorporating artificial intelligence to predict emerging DNS abuse tactics and expanding the database for malicious domain variations. Continuous improvement in response to evolving cyber threats will bolster the system's capability to safeguard users in the digital landscape.

6 Evaluation and Discussion

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

6.1 Confusable Domains

6.1.1 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 in trying to negotiate the hurdles of the digital market and in protecting rights through intellectual property. To navigate these complexities effectively, it is essential to consider several key factors.

- **Commercial Appeal:** High commercial appeal domains are lucrative targets due to the extremely high possibility of attracting a large traffic flow, with potential revenue generation and used for blackmailing purposes in which they demand payment to relinquish the domain. 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 in which they are targeted because they generate huge amount of clicks.

- **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.

6.1.2 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 target , showing ads which bad actors benefit financially from clicks generated by users who visit the site expecting it to be associated with the target , harvesting emails and redirecting to malicious websites.Perhaps the best example in that respect was one of the largest dairy product companies in India, Amul. In the financial year of 2019-2020, the turnover that was brought into account through Amul was staggering, to say the least. During this period, the company was a target for cybersquatting, where some bad actors had registered similar domains impersonating as Amul. These had been used for constructing several phishing sites to further various fraudulent schemes like solicitation for payments under the pretext of distributorship of Amul products and also of securing jobs in Amul. This operation which was active between 2018 and 2020 then finally came down to a public warning and further law actions by Amul to deal with fraudulent activities happening under these domains. Such abuses in the domain name system expose even long-established brands to threats and show the relevance of legal action and public-awareness activities for resolving them ?.
- **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 capitalise on accidental misspellings or phishing attempts that tricked users into visiting ?. An example in December 2020, US healthcare provider Elara Caring suffered a major cyber incident that brought into sharp perspective the vulnerabilities lying at the heart of healthcare's cybersecurity framework. The incident was initiated by gaining unauthorised computer access to email accounts of its staff

and resulted in personal data breaches for more than 100,000 elderly patients. Compromised information included almost every variety of personally identifiable data, from their financial details through to Social Security numbers. The attacker, despite being detected, remained in the system for a week, which may be a signal that the incident response could be better ?.

- **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 ?.

6.1.3 Homograph attacks

The threat of a homograph based attack weaponizing visually similar characters to swindle people persists. This is also true when attackers register domain names to appear like reputable ones, such as when the Latin letter 'l' (lower case "el") is visually confusable with the Latin latter with 'I' (upper case eye), and so on. Such as http://www.paypal.com vs. http://www.paypal.com. Latin character homographs were traditionally used up to now, though with the advent of International Domain Names there are many more possibilities. Although this rising trend suggests a higher potential for such attacks, current data say that they are not very prevalent. Vigilance is, however, important due to the increasing trend in phishing incidents and the ease with which users can be diverted to suspicious sites.

For example, a new study measures homograph attacks on internet users: "Cutting through the Confusion" explains the growth and potential impact of such attacks ?. The current study tries to measure how attackers are able to register domain names having visual similarity with respect to those which are legitimate and authoritative by using confusable characters during phishing. These confusable characters, though seemingly similar to the letters in the authoritative domains, are actually characters different from one another or come from multiple scripts like Cyrillic or Greek, represented in web browsers using punycode to maintain a consistent user experience. This study is summarised in a table of the possible confusable domain names, the count of the actual number of the confusable domain names they found available, and the authoritative domain names. For example, 'yahoo.com' has more than 5000 possible confusables but has been registered two. Another instance is 'google.com', with a thousand possible confusables yet was registered 4. These confusable

domains often contain punycode in their web address, which is not immediately recognised at first glance by the average user.

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

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

Figure 6.1: Registered confusables for popular domains

6.1.4 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 ?. Cloudflare's Zero Trust services enable a proactive approach to blocking confusable domains, which are important to avoid serving phishing sites. In particular, this mitigating measure will be triggered on the first query that involves any domain that is made through the 1.1.1.1 DNS resolver. Such queries will be inspected by the system and checked against a list of possible phishing domains through a "fuzzy" matching protocol. If the domain matches any of the saved patterns for

legitimate brands, then Cloudflare's service would throw an alert. This method used by the server ensures that any domain trying to impersonate a known or respectable brand is detected as soon as it happens in which it provides both real-time monitoring and the capability to search into a historical archive of those domain names, by notifying a security team about new domains observed during the last 30 days that match their saved patterns. This enables a direct review and instant additional taking actions by this domain. The system can also be utilised by Cloudflare for a special investigation in a one-time domain search for some specific domain or pattern, which might become potentially dangerous from a security point of view.

- **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 to determine whether it has mixed script, invisible characters, or visually confusable characters, and whether it is actually validly converted to Unicode. For instance, domains containing characters of different scripts, or those that are clearly identified as mixed script confusables, will be displayed in punycode, warning the users of potential deceptions. Chrome 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. 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.
2. 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.

6.1.5 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 regard to domain abuse threats and trends. Databases and threat

intelligence platforms are shared amongst stakeholders, allowing them to anticipate and avert most such perils well before they impact netizens. This collective effort will enable the formulation of standards by which to coordinate responses to confusable domain incident reports. Mitigating confusable domains 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 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 ?.

Real-life examples of entities seeking to block the resolution of DNS names, especially in connection with public recursive DNS servers, frequently revolve around matters of control, filtering, or securing internet traffic with various kinds of motivations corresponding to such sectors. Some attempted these efforts at the governmental, corporate, and individual levels. As typical examples that pinpoint those instances, consider:

1. Governmental Efforts to Block DNS Resolutions : Governments may interfere directly in the DNS operation to enforce some censorship or block access to particular types of content. For instance, China uses the Great Firewall for regulation concerning access to the World Wide Web within their territory, including doing some mishandling connected with the DNS in order to block out unwanted content ?.

2. Corporate and ISP DNS Filtering : DNS filtering can be deployed by companies and even ISPs in a bid to achieve enhanced online security. For instance, Heimdal Security

explicates how the DNS filtering works as one of the measures for preventing their access to various harmful or inappropriate websites since it first checks the requests for domains. If some are actually flagged, access is denied, hence maintaining both security and productivity within one's organization. This approach is really very effective for the prevention of phishing and malware attacks because it stops the DNS requests towards the malicious sites ?.

3. Ad Block DNS Services : Cloudflare discusses how DNS filtering can be used to prevent access to malicious sites and also filter what is harmful or unfit for viewing. This is done at the DNS level so as to prevent these sites from loading on devices. Cloudflare uses its DNS to filter part of a more prominent policy of access control which is an effort to secure company data and govern what employees will see on the network they manage ? .

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

6.1.6 Techniques for Mitigating Confusable Domains

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

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

1. Registry-Level Measures: Domain registries can implement checks to prevent the registration of domains that are similar to the 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. ?

However, ICANN plays a pivotal role in the detection of confusable domains as it detects confusable domains, especially with respect to Internationalized Domain Names (IDNs) but also it doesn't provide a direct list publication on confusable domain, just like the other gTLD registries. Instead, they tend to develop the frameworks and guidelines for managing the threats related to IDNs and name collisions. This will involve the development of protocols regarding how the processing of internationalized domain names would be done and how the impact that name collisions may possibly have on the domain name system is minimized. ?

People detect on-Internationalized Domain Names (non-IDNs) and Internationalized Domain Names (IDNs) using comprehensive domain, IP, and DNS intelligence tools. Tools which can do so, such as those offered by services like the WhoisXML API, help check domain names for the presence of suspiciously similar domains that could potentially confuse or deceive consumers. An IDN deceptive score is given by means of an algorithm to such types of domains that take into account visual similarities, brand names, and TLD features to see if a domain name is being prepared for deceptive purposes. This approach has proven to be effective in academic research projects at identifying deceptive IDNs over millions of domains distributed across various top-level domains. ?

6.1.7 Technical and Operational Feasibility

The technical feasibility of these techniques varies. Registry-level measures and trademark protection programmes are quite effective, but require cooperation and standardisation across different legal jurisdictions. Automated monitoring is technically feasible and can be implemented on a 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.

6.1.8 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.
- **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.

- **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.

6.1.9 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.

6.1.10 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.

6.1.11 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.

6.2 Phishing

6.2.1 Real-life examples

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

1. InterMed and Spectrum Healthcare Partners fell for a major phishing attack on 44,000 patient data. A Portland-based health care provider, InterMed, could have put the security of 33,000 protected health information (PHI) of its patients at risk due to an attack detected on September 6. Attackers were in the system from September 4 through September 10. The compilation of revealed information included and was not limited to names, dates of birth, health insurance information, and even clinical information accompanied with exposed social security numbers in some cases. In other data breached, Central Maine Orthopaedics issued a report that affected 11,308 patients within their service area by the Spector Healthcare Partners group. Obviously, unauthorized access to emails gives some glimpses about their patient names, date of birth, addresses, and clinical information. This is truly a bad reflection in the middle of an upswing of threats towards health data security, and thus, peremptory steps are required, not just in respect of strengthened security of emails, but in the deep training of support professionals in the best practices ? .

2. In a breathtaking cyber fraud case, both Google and Facebook were almost swindled out of nearly $ 100 million each via increasingly advanced phishing attacks in less than two weeks. In fact, the fake emails were near-identical replicas of real invoices that had been sent by actual suppliers, such that trust and daily procedures were abused in making huge money transfers to fraudster-controlled accounts. This incident is only a portrayal of how susceptible research firms which are highly developed technologically are in the hands of social engineering and thus calling for the tightening of security measures, constant training of the employees, and verification of threats that have

evolved in the cyberspace ?.

6.2.2 Real-life Mitigations

- **Employee Awareness and Training :** Very affirmative in the number of ways a phishing activity is carried out, and the training programme prepared through simulation scenarios for the employees, the Chelsea Technologies employee education policy can be said to be the most significant. It is an inevitable approach, as in most cases, employees contain the credentials and knowledge that drive the breach to succeed. Bringing employees up to date on the different methods of phishing, for example, spoofs and malicious attachments, arms them well in the guarding of sensitive information ?.
- **Comprehensive Security Measures :** LaptopMD points out that the risk of ignorant searching requires the formulation of policies that make it difficult to land on some sites. Besides this, the awareness on the phishers techniques and browsing issues by employees will greatly save them from being caught in cases of phishing ?.
- **Technological and Human Factors :** Each SecureHIM security approach comes with layers of added security in between these, from technological tools such as spam filters and two-factor authentication to staff. It identifies the suspicious link, abstains from clicking on it, and maybe even some browser add-ons that allow one to easily skip some dangerous links. This underscores the fact that technological peripherals and informed employees are crucially needed to provide an effective defence against phishing attacks ?.
- **Awareness against unsolicited emails :** The Center for Democracy and Technology (CDT) outlines some of the best practices in the recognition and act to mitigate phishing; they include the sense of making urgent and unsolicited emails with poor headers, poor links, refusing to reply, open or to click on anything. The next emphasis is to train users on the awareness of phishing by setting avenues for reporting all suspicious messages ?.

6.2.3 Techniques for Mitigating Phishing

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

1. Email Filters: Advanced algorithms are used to identify phishing emails on the basis of a predetermined set of attributes, such as the reputation of the sender, links embedded in the body of the email, and keywords flagged as associated with phishing

are prevented from reaching the inbox.

2. Domain blocking: The first step at an organisational level to make the phishing site not openable by users accidentally is applying domain-blocking measures whether access to the known phishing website from inside an organisation network, this usually inhibits access.

3. User Training: It is important that users are trained directly and to be reminded of any danger they are facing. Training users will require development along the lines of sensing signs in phishing emails, risk taking such as clicking on unknown links, or giving away personal or sensitive information.

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

1. Increasing the Effort for Attackers: Implementing strong authentication methods and encryption to make it more challenging for phishers to access or spoof legitimate websites or email accounts.

2. Clarifying Users' Responsibilities: Educating users about their role in maintaining cybersecurity, including recognising phishing attempts, and reporting them.

3. Enhancing Detection Probability: Utilising advanced detection technologies and threat intelligence to identify and neutralise phishing threats promptly.

4. Limiting Phishers' Access: Restrict the amount of publicly available information that could be used to create convincing phishing emails or impersonating individuals or organisations.

5. Discouraging Future Attacks: Implementing punitive measures against identified attackers and sharing information about phishing campaigns with broader communities to prevent repeat offences.

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

In addition, Phishlimiter ? , which is a new phishing detection and mitigation approach

using Software-Defined Networking where it first proposes a new technique for deep packet inspection (DPI) and then leverage it with software-defined networking (SDN) to identify phishing activities through e-mail and web-based communication.This is how it works :

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

6.2.4 Transparency in Mitigation Efforts

Transparency in cybersecurity, including phishing mitigation techniques, refers to how openly and clearly the methods, policies, and procedures are communicated, understood, and accessible to all stakeholders involved, particularly employees. Here is how transparency can be applied to each of the mitigation techniques described:

- **Employee Awareness and Training :**

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

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

  Having a clear and simple method will inspire the employees to report the false phishing attempts and express their opinions on the training program. It encourages active participation and continuous improvement of the training material.

- **Comprehensive Security Measures:**

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

Justifications: The rationale behind specific policies and restrictions so that the employee will appreciate why they are being put in place does not appear to be a set of arbitrary rules.

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

- **Technological and Human Factors:**

  Tool Transparency: Clearly state the tool and the reason for its being in place for security (e.g., spam filters, two-factor authentication), and its work on subduing phishing. In doing so, such technologization should ideally demystify the trust in these systems.

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

  A Continuous Feedback Loop: Reports and discussions of not only the phishing attempts that technology catches, but also of the ones it misses, have to be actively tracked in order to keep the human element alive in cybersecurity.

- **Awareness against unsolicited emails:**

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

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

  Development of trust: Create an environment where employees will not have any fear of revenge for reporting any insecurity that they might suspect. This can be enabled by an easily established reporting system that is anonymous.

- **Email Filters:**

  The effectiveness of email filtering technology in mitigating phishing attempts is greatly enhanced by transparency about its operational parameters. From disclosing the details of criteria and algorithms it uses to flag warnings over phishing e-mails to such steps as analysis of the reputation of the sender, scanning any content for embedded links and spotting keywords associated with phishing so users can start to

get to grips with how the system makes its decisions. Similarly, an open forum at the beginning of the report that describes how the nature of phishing threats and the evolution of filters to catch them will help users report false positives (legitimate email incorrectly classified as phishing) or false negatives (phishing attempts which get by the filter), can encourage ongoing community participation and, more importantly, help to improve the filtering effort. In an open dialogue about the changing nature of phishing threats and adaptability of the filter in both cases, it engenders trust with the users.

- **Domain Blocking:**

  As a strategy put in place to mitigate access to known instances of phishing sites from within the organisation's network, it gains in the fact that the strategy is transparent by sharing information on criteria and constant update of the blacklist that can help stakeholders understand the reasons leading to the need for access restriction. Create a well-defined mechanism or path for the informer that the site is suspected to be, one which had not been taken into the blacklist, and also a procedure to deny false blockage (like, for example, a legitimate website in case being blocked by mistake). Educating and instructing users, as well as IT professionals, will make them aware of such a measure, and they would be made part of the secure e-culture.

- **User Training:**

  In effect, this means that users are exactly informed about the content and delivery mechanisms of such phishing-focused training programmes. For example, through the inclusion of things such as the types of phishing attacks, an explanation of why certain behaviours must be conveyed-such as the risks of clicking suspicious links, and the psychological tricks of phishers as it means users can be even more informed about the exceptionally high value of the training. Inquiring about the effectiveness of the use of training sessions and what more could be included, that users would prefer to see, will help in making the programs more user-friendly. Such sharing of success stories and statistics, of how those phishing incidents are going down right after the training, are all aspects that could fuel the energy of the employees toward uninhibited engagement and watchfulness in general. Openly discussing the challenge that advanced phishing detection presents and recognising the need for continual educative awareness might really get the ball rolling in the instillation of a culture of security and shared responsibility.

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

  SCP is said to reap tremendous benefit for the transparency of the approach that would be implemented in the means and results. In contrast, through the use of the explanation of how offenders' thinking and environmental stimulation analysis of what

is used to commit phishing attacks are done, the stakeholders could possibly be enlightened on the mitigation means being employed. Useful examples in a showcase format of case studies where SCP strategies were able to defend successfully by increasing the effort and risk to the attacker,attacker, and reducing the potential gain. One could also take feedback from the community on these approaches and elicit suggestions to increase deterrence. This opens up an environment involving continuous development of one's organisation in light of such strategies and other changes.

- **Phishlimiter:**

  Transparency in the use and operation of the newly developed phishing detection and mitigation system is significant towards system acceptance and useful functionality. Detailing the technique of deep packet inspection (DPI) and its integration with SDN to pinpoint phishing activities in email and web communications can demystify the technology for users. By elaborating the criteria and algorithms used to support accuracy in the detection of potential phishing attacks, the strength and reliability of such a system can easily be communicated to stakeholders. The avenue for reporting of the inaccuracies or missed attempts to fish encourages user participation in training the new system. Sharing the progress of Phishlimiter effectiveness with metrics like the number of identified and squashed attacks cements the new-worth technologies on the best ways for handling phishing. Open discussions, for example, on the challenges experienced and in what direction Phishlimiter development has to go, invite greater support from the cybersecurity community to participate in collaboration.

6.2.5 Analysis : What is feasible

1. Employee Awareness and Training : Feasible; Regular training and simulation exercises can be implemented across organisations of any size with scalable online platforms, requiring minimal resources beyond the initial setup.
2. Comprehensive Security Measures :Feasible; The deployment of web filters and secure browsing policies is technically straightforward with existing technology. The main effort lies in continuous policy update and employee education.
3. Technological and Human Factors: Feasible; The integration of spam filters, two-factor authentication, and secure browsing add-ons is readily achievable with current technology. The human element—ongoing employee vigilance—enhances the effectiveness of these tools without significant additional costs.
4. Awareness against unsolicited emails: Feasible; Establishing and communicating best practices for handling suspicious emails involves minimal costs and leverages existing communication channels within organisations.

5. User Training: Feasible; In fact, many of the details about training programmes based on phishing, e.g. information on how content about different methods of phishing, types of attacks, reasons why it is better to look out for who is emailing you, etc., properly belong into our reality. E.g., asking for feedback on how effective is a training program and getting recommended by customers on how to enhance them to make such programs even more user-friendly. Success stories shared and statistics after gamified training sessions motivate and inform. The test is to produce attractive and actual content and to support the process of participation, but it does not seem something excessive.

6. Situational Crime Prevention Approach (SCP): Feasible; SCP approach share insights into the thinking of the offenders as well as into the environmental facilitators to attacks. Offering case studies showing successful impacts of the SCP strategies on deterring of phishing through increased risk and efforts by the attackers can be done. However, sharing in detail the analysis of the offender behaviour may require cautious handling to avoid a 'how-to' guide for potential attackers. Engaging the community for feedback and suggestions is feasible and can foster a continuous improvement environment.

7. Domain Blocking: Moderately Feasible; It is an operational overhead to keep updating blacklists and managing appeals in cases of wrongful blockages. Being able to maintain the updated blacklist and to attend to the appeals in the right manner will have an overhead for the smaller organisation or teams with little resources. Moreover, the evaluation of appeals and requests and the decision process have to be fast, so it cannot always be done with due care and proper research, but sometimes with raw speed.

8. Email Filters: Not Feasible; Although it can certainly be a good idea to describe what type of criteria and algorithms exist for the email filtering process, full disclosure may be too much, because this information will be used, no doubt by the attackers, to make a way around the filters. In fact, in case the attacker is able to fully understand how the mails are actually screened, they can alter their phishing ways to escape from the checkpoints. To some degree, transparency is possible, although full revelation of all operating parameters would represent a type of chaos where spam would just explode right through.

9. Phishlimiter: Not Feasible; With the technical technologies as Deep Packet Inspection (DPI) and Software-Defined Networking (SDN), the complexity in Phishlimiter is at a higher level, maybe containing sensitive, proprietary security information. These three above would at best not be achieved without a fear of marking being compromised; background on the specifics of such technologies and testing on how they are

integrated for phishing detection is technically too complex to summarise. Finally, the evolving and relatively complicated unpredictable tactics used by phishing attackers around the globe would demand that Phishlimiter therefore keep pace with the developments, and those making changes have to ensure that, at every point in time, it keeps up with current events, which sometimes may be difficult to disclose in real time without the adversaries having a foothold.

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

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.