

# Understanding the Economic Impact of Botnets in Bangladesh: Insights and Strategies from Attacker & Victim Perspectives

by

Rodoshie Reheean  
21301417

Golam Sarwar Sami  
21101276

Syeda Ifroza Ahmed  
21301470

Anonna Dev Nipa  
21301191

A thesis submitted to the Department of Computer Science and Engineering  
in partial fulfillment of the requirements for the degree of  
B.Sc. in Computer Science

Department of Computer Science and Engineering  
Brac University  
October 2024

© 2024. Brac University  
All rights reserved.

# Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

**Student's Full Name & Signature:**

---

Rodoshie Reheean  
21301417

---

Golam Sarwar Sami  
21101276

---

Syeda Ifroza Ahmed  
21301470

---

Anonna Dev Nipa  
21301191

# Approval


The thesis/project titled “Understanding the Economic Impact of Botnets in Bangladesh: Insights and Strategies from Attacker & Victim Perspectives” submitted by

1. Rodoshie Reheean (21301417)
2. Golam Sarwar Sami (21101276)
3. Syeda Ifroza Ahmed (21301470)
4. Anonna Dev Nipa (21301191)

Of Summer, 2024 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on October 17, 2024.

## Examining Committee:

Supervisor:  
(Member)



---

Md Faisal Ahmed  
Lecturer  
Department of Computer Science and Engineering  
Brac University

Co-Supervisor:  
(Member)

---

Dr. Md Sadek Ferdous  
Associate Professor  
Department of Computer Science and Engineering  
Brac University

Head of Department:  
(Chair)

---

Dr. Sadia Hamid Kazi  
Chairperson and Associate Professor  
Department of Computer Science and Engineering  
Brac University

# Ethics Statement

All of the necessary steps were taken to make sure that the research process adhered to ethical considerations, including but not limited to the following:

1. **Informed Consent:** Participants involved in the surveys and interviews were properly informed about the purpose of the research and how their data would be used. Their participation was entirely voluntary. Consent was obtained before collecting any data.
2. **Data Confidentiality and Anonymity:** All data including personal and sensitive, were collected anonymously ensuring participants confidentiality and were securely stored. All efforts were made to preserve the identity of the participants ensuring that no sort of identification was disclosed at any part of the research.
3. **Compliance with Applicable Laws and Regulations:** The research was conducted in full compliance with legal requirements and institutional guidelines. No data collection or analysis has violated national or international data protection laws and regulations.
4. **Research Integrity:** The authors affirm that all data presented is valid and accurate. All findings are original and no fabrication or falsification, or plagiarism was involved in conducting or presenting this research. Proper citations have been provided wherever external work has been referenced.

By adhering to these guidelines, this research maintains the highest standards of ethical integrity.

# Abstract

Botnets pose a significant threat to Bangladesh's cyberspace and to its economic stability, especially in critical sectors such as finance, government and technology. This research investigates the life cycle and economic impacts of botnets in Bangladesh from multiple perspectives namely the attacker, the general public, and security experts. It explores how botnets target vulnerable systems, the methods and strategies used by attackers to propagate botnets and the financial and operational harm they pose to organizations. Data was collected through surveys targeting both attackers and victims, and also via interviews with cybersecurity professionals to identify effective detection and mitigation strategies. The research findings reveal substantial financial losses due to botnet attacks and emphasizes the need for a robust cybersecurity framework tailored for Bangladesh's evolving digital landscape. The proposed framework aims to prevent digital casualties for the general public, minimize botnet-related activities and economic disruptions in government institutions and financial sectors.

**Keywords:** Botnets, Cybersecurity, Botmasters, Economic Impact, Financial Sectors, Bangladesh, Cybersecurity Framework

## **Acknowledgement**

Firstly, all praise to the Almighty because of whom our thesis have been completed without any major interruption.

Secondly, to our Advisor Md Faisal Ahmed & Co-Advisor Dr. Md Sadek Ferdous for their kind support and advice in our work. They helped us whenever we needed. We would also like to acknowledge the contributions of the Chief Technology Officer, A.S.M Shamim Reza and the Marketing Manager, Md. Mazharul Islam from Pipeline Inc. for their valuable insights.

Lastly, we are thankful to our parents for supporting us throughout.

# Contents

<b>Declaration</b>	<b>i</b>
<b>Approval</b>	<b>ii</b>
<b>Ethics Statement</b>	<b>iii</b>
<b>Abstract</b>	<b>iv</b>
<b>Acknowledgment</b>	<b>v</b>
<b>List of Figures</b>	<b>ix</b>
<b>List of Tables</b>	<b>x</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Motivation . . . . .	2
1.2 Research Problem . . . . .	4
1.3 Research Objectives . . . . .	6
1.4 Report Structure . . . . .	6
<b>2 Background</b>	<b>8</b>
2.1 Botnet Overview . . . . .	8
2.1.1 History and Evolution of Botnets . . . . .	8
2.1.2 Economic Aspects of Botnets . . . . .	9
2.1.3 Botnet History in Bangladesh . . . . .	10
2.2 Life Cycle of Botnet . . . . .	11
2.2.1 Initial Infection . . . . .	11
2.2.2 C&C Establishment . . . . .	12
2.2.3 Propagation and Expansion . . . . .	14
2.2.4 Execution of Malicious Activities . . . . .	15
2.2.5 Maintenance and Updates . . . . .	16
2.2.6 Detection and Mitigation Avoidance . . . . .	16
2.2.7 Retirement . . . . .	17
<b>3 Literature Review</b>	<b>21</b>
<b>4 Methodology</b>	<b>27</b>
4.1 Victim’s Perspective Survey . . . . .	27
4.2 Attacker’s Perspective Survey . . . . .	28
4.3 Semi-structured Interview with Cybersecurity Professionals . . . . .	29

4.4	Exploratory Data Analysis . . . . .	29
4.5	Hypothesis Testing . . . . .	30
<b>5</b>	<b>Victim’s Perspective</b>	<b>33</b>
5.1	Data Analysis for Victim’s Perspective . . . . .	34
5.1.1	Demographics . . . . .	34
5.1.2	Online behavior . . . . .	36
5.1.3	Cybersecurity Incidents by Device and Connection Type . . . . .	36
5.1.4	Awareness and Security Measures . . . . .	38
5.1.5	Practices and Concerns . . . . .	39
5.2	Hypothesis Testing for Victim’s Perspective . . . . .	41
5.2.1	Experimental Design . . . . .	42
5.2.2	Study Objectives . . . . .	42
5.2.3	Hypotheses . . . . .	42
5.2.4	Results and Analysis . . . . .	42
<b>6</b>	<b>Attacker’s Perspective</b>	<b>50</b>
6.1	Data Analysis for Attacker’s Perspective . . . . .	50
6.1.1	Attackers on Goals & Target Selection . . . . .	51
6.1.2	Attackers on Information Gathering . . . . .	54
6.1.3	Financial Aspects . . . . .	56
6.1.4	Operational Techniques and Adaptability . . . . .	58
6.2	Hypothesis Testing for Attacker’s Perspective . . . . .	60
6.2.1	Experimental Design . . . . .	60
6.2.2	Study Objectives . . . . .	61
6.2.3	Hypotheses . . . . .	61
6.2.4	Results and Analysis . . . . .	61
<b>7</b>	<b>Security Expert’s Perspective</b>	<b>68</b>
7.1	Overview of Botnet Detection and Defense . . . . .	68
7.2	Challenges in Botnet Mitigation and Cybersecurity Preparedness . . . . .	69
7.3	Financial and Operational Impact of Botnet Attacks . . . . .	69
7.4	Key Components for a National Cybersecurity Framework . . . . .	69
7.5	Recommendations for Enhancing Cybersecurity in Bangladesh . . . . .	70
7.5.1	People and Technology Insights . . . . .	70
7.5.2	Technological Innovation and Automation: . . . . .	70
7.5.3	Improving Law Enforcement Collaboration: . . . . .	71
7.6	Conclusion and Policy Implications . . . . .	71
<b>8</b>	<b>Analysis &amp; Discussion</b>	<b>72</b>
8.1	South Asia vs Bangladesh Comparison . . . . .	72
8.2	Global vs Bangladesh Comparison . . . . .	74
8.3	Key Findings and Discussion . . . . .	78
<b>9</b>	<b>Technical Evaluation</b>	<b>80</b>
9.1	Technical Evaluation of Existing IDS/HIDS Tools . . . . .	80
9.2	Snort . . . . .	80
9.3	Suricata . . . . .	84
9.4	OSSEC . . . . .	86



9.5	Integrated Solution: Combining Snort and Suricata . . . . .	86
<b>10</b>	<b>Proposed Framework for Bangladesh</b>	<b>91</b>
10.1	Existing Cybersecurity Framework of Bangladesh and its Gaps . . . . .	91
10.2	Security Experts' Recommendations: Focus on People, Process, and Technology . . . . .	92
10.3	Learning from Singapore: A Model for Bangladesh . . . . .	94
10.4	Proposed Framework for Bangladesh: People, Process, and Technology . . . . .	95
<b>11</b>	<b>Conclusion and Future work</b>	<b>98</b>
	<b>Bibliography</b>	<b>101</b>
	<b>Appendix 1</b>	<b>106</b>
	<b>Appendix 2</b>	<b>109</b>

# List of Figures

2.1	Life Cycle Of A Botnet . . . . .	14
2.2	Mirai Botnet Timeline . . . . .	19
4.1	Methodology Flowchart . . . . .	32
5.1	Experience of Cybersecurity Incidents . . . . .	34
5.2	Botnet Familiarity . . . . .	35
5.3	Distribution of Time Spent on the Internet Each Day . . . . .	36
5.4	Cybersecurity Incidents by Device, Internet Connection Type and Incident Status (Log Scaled) . . . . .	37
5.5	Familiarity with Botnets Based on Cybersecurity Education . . . . .	38
5.6	Heatmap of Update Frequency vs. Cybersecurity Awareness . . . . .	39
5.7	Action Taken When Malware is Suspected . . . . .	40
5.8	Influence of fear of botnet attacks . . . . .	41
6.1	Botnet Attack Distribution in South Asia . . . . .	51
6.2	Targeted Entities for Botnet Inclusion . . . . .	52
6.3	Distribution of Primary Goals For Launching Botnet Attacks . . . . .	53
6.4	Propagation Tactics Used By Attackers Who Launch Trojan Attacks . . . . .	54
6.5	Proportion of Attackers Gathering Info on Cybersecurity Trends . . . . .	55
6.6	Information Sources for Local Botmasters . . . . .	56
6.7	Primary Monetization from Botnet Attacks . . . . .	57
6.8	Monthly Income Range From Selling Stolen Data . . . . .	58
6.9	Propagation Distribution for Drive-by-Downloads . . . . .	59
6.10	Tactics for Adjusting to Security Measures . . . . .	60
8.1	Botnet Attack Distribution Bangladesh Vs South Asian Countries . . . . .	72
8.2	Targeted Entities Distribution Bangladesh Vs South Asian Countries . . . . .	73
8.3	Comparison Chart of Money Generated By Botnet Attacks Bangladesh Vs South Asian Countries . . . . .	74
9.1	Server Performance During ICMP flood. Before vs After Snort . . . . .	82
9.2	Server Performance During ICMP flood. Before vs After Suricata . . . . .	85
9.3	Server Performance During DDoS attack Before vs After Snort + Suricata . . . . .	88
10.1	Proposed Framework For Bangladesh . . . . .	97

# List of Tables

3.1	Literature Review Summary (Part 1)	25
3.2	Literature Review Summary (Part 2)	26
5.1	Demographics of Survey Respondents	33
5.2.1	Contingency Table of ‘Awareness of Botnets’, ‘Updates Software’, and ‘Willingness to Spend Money’	43
5.2.2	Observed Frequencies for variables ‘Awareness of Botnets’ and ‘Updates Software’	44
5.2.3	Expected Frequencies for variables ‘Awareness of Botnets’ and ‘Updates Software’	44
5.2.4	Observed Frequencies for variables ‘Awareness of Botnets’ and ‘Willingness to Spend Money’	45
5.2.5	Expected Frequencies for variables ‘Awareness of Botnets’ and ‘Willingness to Spend Money’	45
5.2.6	Observed Frequencies for variables ‘Updates Software’ and ‘Willingness to Spend Money’	45
5.2.7	Expected Frequencies for variables ‘Updates Software’ and ‘Willingness to Spend Money’	46
5.2.8	Contingency Table of ‘Staying Informed’ and ‘Downloads Cracked Software’	47
5.2.9	Expected Frequencies for variables ‘Staying Informed’ and ‘Downloads Cracked Software’	47
6.2.1	Contingency Table of ‘Target’, ‘Primary Investment’, and ‘Use of Evasion Tactics’	62
6.2.2	Observed Frequencies for variables ‘Target’ and ‘Primary Investment’	62
6.2.3	Expected Frequencies for variables ‘Target’ and ‘Primary Investment’	63
6.2.4	Observed Frequencies for variables ‘Target’ and ‘Use of Evasion Tactics’	63
6.2.5	Expected Frequencies for variables ‘Target’ and ‘Use of Evasion Tactics’	63
6.2.6	Observed Frequencies for variables ‘Primary Investment’ and ‘Use of Evasion Tactics’	64
6.2.7	Expected Frequencies for variables ‘Primary Investment’ and ‘Use of Evasion Tactics’	64
6.2.8	Contingency Table of ‘Monetization Methods’ and ‘Monthly Earnings in BDT’	66
6.2.9	Expected frequencies for variables ‘Monetization Methods’ and ‘Monthly Earnings in BDT’	66
8.2.1	Comparison of Attacker Perspectives: Bangladesh vs Global	75
8.2.2	Comparison of Public Perspectives: Local vs Global	77
8.2.3	Comparison of Security Expert Perspectives: Local vs Global	78
9.2.1	System Performance Before and After Enabling Snort during ICMP flood attack	82
9.3.2	System Performance Before and After Enabling Suricata during ICMP flood attack	85

9.5.1 System performance comparison during a DDoS attack before and after running Snort and Suricata. . . . .	88
---	----

# Chapter 1

## Introduction

In recent times, the usage of technology has increased exponentially in different fields in the digital landscape of Bangladesh. Especially businesses and individuals have adopted the usage of technology in many aspects, contributing to the economy of the country. But with this rapid growth of digitalization, the threat of cybercrimes comes along. As a result, it poses a sequence of serious threats for organizations and individuals relying on technology for their daily lives. Among those threats, botnets pose a high risk to a country's economic prosperity.

Botnets, which are networks of infected devices controlled remotely by malicious actors can amplify the severity of cybersecurity threats which is why it constitutes a substantial security challenge. Botnets are often used to launch DoS (Denial of Service) attacks and distribute malware and phishing links. Moreover, it can also be used to exploit devices to steal sensitive data, and also to use the infected network of devices to mine for cryptocurrencies. It even goes beyond technological disruption as it has negative effects on financial aspects, disrupts organizational processes and discourages Internet-based organizations.

Understanding how botnets impact the economy from different perspectives and fields of work is crucial for developing effective strategies to mitigate their impacts. This research delves into various aspects of botnet's operational principles in Bangladesh. It provides a valuable insight into the adverse effect of botnets in cyberspace and to the economy of the country. Aspects such as why attackers target, their motive, the vulnerabilities they exploit, the organizations they target and the strategies that have successfully mitigated the risk of botnets have been discussed in this research. The goal of the research is to uncover the substantial financial impact due to botnets by investigating the life-cycle of botnets starting from the initial infection to retirement as well as how they spread.

This study collected data from three key groups-attackers, the general population, and cybersecurity experts within Bangladesh to form a comprehensive view of botnet operations and their economic implications. Survey was taken targeting local attackers that provided insights into their strategies, motives and their methods of operations. This allowed the research to develop some crucial hypotheses that describe the dangers posed by botnets and unveil the vulnerabilities attackers exploit. Moreover, data from the general population was collected through an extensive

survey to assess public awareness, behaviors and the vulnerabilities exploited by botmasters in Bangladesh. This survey targeted a wide range of demographics including students, professionals, and non-technical users. This helped gain valuable insights into how individuals interact with technology and where they are most vulnerable to threats related to botnets. Furthermore, semi-structured interviews with cybersecurity professionals offered expert opinions and views on the cyberspace landscape of Bangladesh and on current detection and mitigation strategies. Another major contribution of this study was highlighting the comparison of primary research and secondary research, as well as, evaluating the existing intrusion detection systems such as Snort, Suricata, and OSSEC in mitigating botnet attacks. This evaluation helps identifying the effectiveness and limitations of these tools in real world scenarios.

This multi perspective data collection provides a holistic understanding of the digital threats which allows the creation of cybersecurity strategies tailored for Bangladesh. The hypotheses and data acts as the backbone or framework of reference to unlock the relationship between botnets and the economy of Bangladesh.

As Bangladesh heads on its journey towards a futuristic tech vision, protecting against botnet attacks is a huge and crucial task. The purpose of this study is to uncover the life-cycle of botnets to understand them, while also to dig out the financial influence they have on Bangladesh. Thus, by gaining key insight from attackers, the general population, and cyber security experts the financial impact of botnets has been uncovered and a solid framework to safeguard Bangladesh's cyberspace and financial sectors has been proposed in this research.

## 1.1 Motivation

Bangladesh has been through a transformative experience in the digital realm. Along with successful tech advancement, it has also seen a growth of attacks in cyberspace. Within this context, the BGD e-GOV CIRT has identified a spectrum of botnet attacks targeting critical sectors, such as government, financial, military, industrial, trade and commerce, healthcare, start-up and innovation, and the energy sectors of Bangladesh [6]. The looming threat of cyber attacks has put forward significant challenges ahead for the country, as cybercriminals mostly target data that is confidential, sensitive, personal, and financial [29]. These attacks not only compromise the virtual walls but also, most importantly, have a real economic impact, threatening the country's financial well-being and the economy as a whole. Despite such high risk, data are scarce due to inadequate collaboration and research. The data is necessary to protect government institutions, especially the financial technology domain. It is predicted that Bangladesh will likely face an increasing number of cyber-attacks in the near future [29]. This study takes a deeper dive into uncovering a solution to combat botnet attacks that further looks into the economic repercussions, from multiple perspectives like the general mass, attackers, and security professionals in an effort to defend the institutes. Therefore, this research topic provides thought-provoking insights and facts into the world that revolves around critical sectors as well as the economic aspects of Bangladesh that come along.

According to [28], the financial technology sector has experienced rapid and exponential growth in recent years, in Bangladesh. It has revolutionized the ways of providing financial services across businesses, economics and various other domains. It has the ease of accessibility and convenience, lower costs, innovation and efficiency, and financial inclusion. Apart from all these benefits, the financial sectors do face cyber threats due to their heavy reliance on technology and financial data [29]. Both of these can be manipulated and thus, are quite sensitive. Moreover, cyber security breach incidents will have a damaging impact on financial institutions as well as the broader economy as large sums of money are compromised during these cyber attacks. So, effective measures for the digital landscape are necessary to maintain the requirements and trust of customers. In addition, as the number of people having access to the internet in Bangladesh is growing, the financial sectors have an opportunity to grab a wider customer base [29]. Hence, financial institutions like Bkash, Nagad, etc. have been proven to be successful in their ventures amongst the Bangladeshi people, but with danger lurking around. According to [30], in the 21st century, online banking heists and data leak incidents are two of the most significant threats a country can face. This can be achieved through phishing emails, malware, botnets, and hacking into the vulnerable system itself. Over the years, several financial institutions have faced cyber attacks which signifies how important it is to implement security measures in this critical sector.

On February 7th, 2016 Bangladesh witnessed the largest online banking burglary where they almost lost 951 million dollars due to the theft [31]. The employees at Bangladesh Bank noticed something was wrong when their main printer stopped working for a few days. However, when they managed to get it back to working they saw 35 fraudulent transfer requests worth millions of dollars. All the transactions were unauthorized and made under their radar even bypassing the SWIFT system. Out of that 951 million dollars, 850 million was blocked by the Federal Reserve Bank of New York. However, 81 million dollars were successfully transferred to accounts in the Philippines [31].

In addition, Nagad-a financial institution based in Bangladesh, had a massive data leak incident earlier in 2024 [32]. Nagad is one of the key institutions in the country's digital finance. With a user base exceeding over 81 million registered users which is nearly half the population of the country [32]. Nagad processes daily transactions that go beyond BDT 1,300 crores (\$111 million), according to a 2023 Nagad press release [32]. This company has gained numerous awards and recognition's, named such as being named the "Fastest to Unicorn" for achieving a valuation of over \$1 billion in record time. Nagad also received accolades for its innovative payment solutions and contributions to financial inclusion [32]. Despite its scale and success, vast amounts of user data from Nagad including NID number, name, date of birth, father and mother's name and even their address were leaked [32]. This incident underscores the challenges and vulnerabilities faced by giant financial institutions due to digital threats. Which affects the trust of millions of users and also potentially jeopardizes the integrity of financial transactions across the whole nation. Along with Nagad, NID of Bangladesh was affected as well as some other entities whose identities were kept a secret. The BGD e-GOV CIRT alerted them. Details of this incident are discussed in Chapter 2.1.6 Botnet History in Bangladesh.

From these incidents, it can be understood how important it is to protect the financial sectors to safeguard the national wealth. Therefore, it is important to understand what went wrong and how stronger security measures can be implemented. First and foremost, it is notable from the Bangladesh bank heist that cybersecurity training is required to ensure that the human factor is ensured to be safe from phishing attacks. The staff must learn about social engineering and how to stay away from clicking on just any random link without verifying.

Presently, the Bangladeshi cybersecurity landscape and the economic aspects related to it stand at a precarious ground as seen from the perspective of both the general public and an attacker. Significant research has not been carried out regarding the severe consequences of such attacks. Currently, there is no specific solution to botnet attacks in Bangladesh however, the present cybersecurity framework does offer a reactive approach. Although reactive measures can offer solutions to respond to an attacker but it isn't adaptive. The research [45] explores the disruptive nature of botnets and develops a framework by analysing both human and technological aspects of such attacks which contributes by enabling a dynamic understanding and improving defense strategies against cyber threats. In order to prevent botnet attacks, it is vital to implement a proactive approach that welcomes change. It is impossible to protect critical sectors against this evolving threat with reactive measures. This is where this particular research work becomes relevant and necessary. It brings along valuable opinions, suggestions, and comments from multiple viewpoints of attackers, common people, and security professionals. These valuable insights obtained, assist in further analyzing the extent of financial impairment in Bangladesh due to cyber attacks like botnet attacks. It also points at the specific areas of cybersecurity in the financial sectors that need to be focused upon so that they are better able to defend themselves from any cyber attacks in the long run. Therefore, there is a necessity for a proactive framework that will be used to meet the needs of defence methods from heinous botnet attacks, and eventually assist in reducing the risk of being targeted by botnets. That is why, while designing the framework the financial sector was chosen, more specifically the government-funded financial institutes, keeping in mind the at-risk cyber landscape and the economic challenges that come along with digital Bangladesh. Thus, this study is valid and important as it enlightens the lesser-known paths by crucially contributing to both the financial industry as well as cybersecurity, in the context of Bangladesh. Moreover, the survey data collected not only provides valuable information about the local botmasters on their incentives, operation tactics, targets, and monetization but also valuable insights gathered from general public's awareness, internet usage, and experience. These datasets bring contribution to aid in future research as well.

## 1.2 Research Problem

The evolving landscape of cyber threats, especially botnets pose a significant challenge to the security of Bangladesh's digital domain. This is even made more complicated by the fact that the ongoing geopolitical threat affects the entire world and extends its impact to Bangladesh, making it even harder to secure its cyberspace [6]. Within this context, the BGD e-GOV CIRT has identified a spectrum of botnet at-



tacks targeting critical sectors, such as government, financial, military, industrial, trade and commerce, healthcare, start-up and innovation, as well as the energy sectors of Bangladesh [6].

These attacks not only compromise the virtual walls but also, most importantly, have a real economic impact, threatening the country's financial well-being and the economy as a whole. One of the major barriers that have been identified relating to cybersecurity in Bangladesh is the lack of encouragement to report cyber incidents due to the stigma associated with it. In Bangladesh, with a population of 172.95 million, 522 cybercrime cases were reported in 2022, translating to 0.30 reports per 100,000 people. However, the actual number of cases is estimated to be 3,480 which suggests that many incidents go unreported. The estimated financial loss from the 522 known cases was \$4.21 million but if estimated 3,480 cases are considered, the financial losses could reach up to \$28.08 million [58]. According to [6], victim shaming is the biggest fear that discourages institutions to report any incident. This fear underlines a reluctance of entities to immediately report cyber incidents to the national incident response team. This reduces the ability to collectively react to such incidents and possibly reduce potential economic losses [6].

Bangladesh experienced a horrific economic impact in 2019 from an incident of cyber threats in which three local private banks suffered major cyber-attacks. Hackers exploited vulnerabilities in the banking infrastructure, stealing up to USD 3 million from cash machines located in Cyprus, Russia, and Ukraine, using cloned credit cards [6]. This incident highlights the urgency for extensive defensive strategies tailored to the specific vulnerabilities inherent in Bangladesh's digital systems.

Furthermore, the BGD e-GOV CIRT's discovery of 3,639 bank cards issued by different Bangladeshi Banks on the dark web emphasizes the gravity of the situation. The urgency of reinforcing the cybersecurity framework is further emphasized when vulnerabilities within the banking infrastructure were identified. To protect Bangladesh's digital assets and lessen the economic impact, amplified cybersecurity measures will help [6].

Thus, the aim of the research is to answer this question:

***How can Bangladesh enhance its cybersecurity framework to mitigate the economic impact of botnet attacks targeting financial sectors?***

To answer this question, the research will therefore strive to explain the losses that botnets cause in Bangladesh by examining the viewpoints of the attackers and general public's. To this end, with the help of conducting an interview with security experts and analyzing the general picture of Bangladesh's digital security situation, the study aims to outline the concrete threats that have been revealed in the country's digital environment, as well as develop the corresponding protective measures that would help the country to become more prepared for the potential cyber-attacks.

## 1.3 Research Objectives

This research aims to develop a defensive framework to protect Bangladesh's digital landscape from botnet attacks. The objectives of this research are:

1. Understanding the botnet life-cycle from its initial infection to retirement.
2. Exploring the reasons or motivations behind botnet attacks by analyzing the attacker's perspective.
3. Investigating the economic impacts of botnets on the financial sectors in Bangladesh.
4. Assessing the challenges and effectiveness of current detection and mitigation efforts that are put in place by cybersecurity agencies, while also evaluating existing mitigation tools, strategies and identify prevention measures to minimize the economic impact of botnets in Bangladesh.
5. Establishing a comprehensive defensive framework for Bangladesh against botnets.

## 1.4 Report Structure

- Chapter 2: Presents Background where overview of botnet, its history and evolution, economic aspects, botnet history in Bangladesh, and botnet life cycle have been discussed.
- Chapter 3: Outlines related works on botnets and comprehensive literature review.
- Chapter 4: Outlines the methodology, detailing the survey data collection process, the analysis of both attacker and general public perspectives, the approach used for conducting interviews with security experts, and the methods employed to analyze the collected data.
- Chapter 5: Explores Victim's Perspective where online and economic behavior of the general populace within Bangladesh are analysed.
- Chapter 6: Exhibits Attacker's Perspective, exploring the mindset of botmasters, highlighting their motives and operational trends.
- Chapter 7: Maps out Security Expert's Perspective, uncovering the tactics and preventive measures taken by the country's security experts to fight against botnet attacks.
- Chapter 8: Presents Analysis & Discussion, highlighting key findings and connects all three perspectives.
- Chapter 9: Outlines Technical evaluation where existing open source IDS tools are evaluated and solutions are proposed for improvement.
- Chapter 10: Defines Proposed Framework for Bangladesh which elaborates on how to stay protected from botnet attacks.

- Chapter 11: Summarizes Conclusion and Future work where the thesis work was concluded and scope of future works were mentioned.

# Chapter 2

## Background

This chapter examines botnets, their history and evolution, propagation methods, economic impacts and the life cycle of botnet. It delves into botnet history globally as well as in Bangladesh. Moreover, discusses how bot binaries including worms and trojans, spread through malicious processes and how they establish connections with their control servers. It also highlights the economic impacts of botnets, detailing direct financial losses from extortion and fraud, as well as the broader repercussions for governments and businesses. Understanding these aspects is crucial for developing effective cybersecurity strategies and safeguarding the cyberspace of Bangladesh.

### 2.1 Botnet Overview

A botnet is a network of devices infected with malicious software. They are collectively controlled without the awareness of their owners. The botnet is controlled by the “Botmaster” or “Bot herder” and each of the infected devices in the network is called a “bot” or a “zombie”. The botmaster is the controller of the botnet and they are responsible for creating, maintaining and controlling the network of bots. Using various methods, the botmaster issues commands to the bots to do malicious tasks such as sending spam emails, spam campaigns, crypto mining, DDoS attacks, stealing data and installing additional malware [8]. Due to the infected devices being a part of the centralized system, the botmaster has overall control over it. It can ultimately execute attacks on a larger scale that would not have been possible with the usage of a single computer or device.

#### 2.1.1 History and Evolution of Botnets

Botnets have evolved quite significantly since their first appearance. The first recognized botnet, “Sub7” emerged in the late 1990’s allowing attackers to take over control of infected machines remotely [49]. Over the years, botnets have evolved and more harmful functionalities have been added. Botnet variants such as Mirai and Emotet are prime examples of botnets’ advanced capabilities and their complex defence mechanism against take-down efforts.

## 2.1.2 Economic Aspects of Botnets

To find out the full scope of botnet impact on the economy as well as the society, it is important to understand the economic aspects of botnets. Contributing to incentives, broader comprehension of the costs, and influences associated with botnet activities, these economic aspects go beyond several facets [1].

- **Direct Financial Aspect:** The direct financial influence of botnets on businesses, individuals, and governments is a primary aspect. Botnets can cause significant financial losses through malicious activities like extortion, fraudulent transactions and stealing of private information. As a consequence, individuals may suffer from identity theft, unauthorized access to private accounts, or loss of personal funds. It can also cause massive damage to businesses as well. For example, financial loss, loss of customer data, intellectual property, reputational damage, and operational disturbances can cause significant damage.
- **Government Economic Repercussions:** The economic repercussions that the Governments have to deal with are in terms of lost tax revenue and damage to critical infrastructure [6]. Additionally, botnets can contribute to large-scale economic impacts at both national and global levels. Due to the botnet effect, there is less participation in e-commerce and digital services as the fear of botnets break the trust of people from such platforms. This causes many e-commerce services to be rendered useless as the consumer has no trust in online transactions. Due to this, the growth of the economy among the digital industry gets negatively affected [6].
- **Criminal Activities and Revenue Generation:** There are numerous and ever-changing purposes from an economic angle to botnet activities. Currently, the attackers make their income performing criminal activities such as selling stolen data in the black market or leasing botnets for DDoS attacks on a competitor platform, mass mining bitcoins etc. To counter these, one needs to look into botmasters' behaviors and intentions. Using these, an adequate organizational outline can be constructed to counter botnet processes and dismantle its socio-economic industry.

Given this, it can be argued that due attention should be paid to the economic effects of botnets because they reveal various positive and negative effects of botnets in all sectors. Through understanding the economic motivations that result in botnet activities, cybersecurity professionals and agencies can develop more tailor-made targeted strategies to mitigate the threat posed by botnets and help keep digital infrastructures safe and secured. As botnets pose a significant threat in cyberspace it is required to understand the incentive to develop effective defenses against it. As technology evolves, so do the sophistication and risks associated with botnets, necessitating continuous adaptation in cybersecurity strategies.

### 2.1.3 Botnet History in Bangladesh

A cyber-espionage group, APT28, also known by Pawn Storm, Fancy Bear and others, is a supposedly Russian state-sponsored group that has carried out cyberattacks actively since 2007 [33]. They use different tools and methods and have different motives for the attacks. It was revealed in 2014, that there exists another cyber security breachers team who launched a campaign primarily targeting the US Senate and Democratic National Committee [33]. They used malware and spear-phishing in the campaign. They also created fake Outlook Web Access login pages for phishing credentials and for mobile device attacks. Along with that, they developed iOS malware. The documents that were stolen were published in October and November by WikiLeaks [33].

Diving deeper into botnet attack history in financial institutions all over the world, some details were uncovered successfully. According to [34], in 2017, several reports of security breach incidents within financial institutions were made. The websites of banks were locked using malware like WannaCry, Petya, and BadRabbit [34]. The attackers also made use of botnets, along with others such as DDoS attacks, phishing, etc. As per reports by the Gray Wizard, which registered 167,324,652 incidents, most of the security attackers were targeted towards websites that belonged to France, next in place came Great Britain, then an increasing record of traffic came from Germany, the United States, and Poland as well [34]. In the same way, Bangladesh has also faced numerous cyber attacks, according to Bangladesh state-run e-Government Computer Incident Response Team (BGD e-GOV CIRT) under the Ministry of Posts, Telecommunications and Information Technology [6]. While the number of such registered incidents was the highest at 1154 in 2020, it declined over the years, to 185 as reported in 2023 [6]. These security breach incidents have been classified into two categories - vulnerability of the system and intrusion attempt. Most of the cases arose due to a vulnerable system, as evident in the statistics report of the national website of Bangladesh.

In addition, Nagad-a financial institution based in Bangladesh, had a data leak incident earlier in 2024. They have over 80 million registered users and their transactions go beyond \$111 million, according to a 2023 Nagad press release. Along with Nagad, NID of Bangladesh was affected as well as some other entities whose identities were kept a secret. The BGD e-GOV CIRT alerted them. One of the leading newspapers of Bangladesh, The Daily Star reported that users having Nagad accounts had their data leaked across Telegram bots. It was examined further to discover from the reports that, with just a mobile phone number it was possible to pull out an individual's personal information from a Telegram bot, one telegram channel that was operated by humans, and a website. Starting from November 2023 till January 31, 2024, the telegram bot, telegram channel, and website were created [35]. The bot supplied information free of cost, on the other hand, the website provided half of the information at no cost but for the other half, charged a subscription fee of 640 Bangladeshi Taka. All of this actively ran until March 6, 2024 [35]. The extracted information included NID number, name, birth date, mother's name, father's name, and address but they were not able to get access to the transaction data of customers [35]. Every piece of data being shared in the telegram channels and via bots was public, so it was accessible to everyone within the groups [35]. However,

it was not possible to uncover who was behind this as all information was encrypted.

In line with the telegram channels' claims, it was able to fetch the data from the "Know Your Customer" database, otherwise known as KYC. It is a step required to be completed by the customers for a functioning account. For completion, the user needs to upload a scan of their NID, and then the app extracts relevant data from the scanned copy and fills the customer's Nagad profile automatically. The KYC database also stores photos of the user but the telegram website and bots involved, could not return those along with all other information. Under Bangladesh Mobile Financial Services Regulations 2022, completion of this step is mandatory.

On the other hand, when asked, Nagad deemed the whole incident a "smear campaign" and denied all claims [35]. According to [35], this specific incident is linked to other citizen data leaks that happened back in 2023, particularly from the government's land tax portal. Furthermore, based on the Bangladesh data protection bill all of the leaked data, from the telegram bot, channel, and website are classified as personal data. In addition, the National Cyber Security Index as per the 2024 update, reported that Bangladesh has a zero score in protecting personal data. However, Bangladesh has a high score on "cyber incident response", therefore standing at 24 globally. As a result, it is evident and indicative of how ineffectively these cyber security breaches and incidents are handled in the digital landscape of Bangladesh.

In conclusion, the dark history of numerous attacks has taken Bangladesh by storm. The recent 2024 Nagad incident is a prime example of such heinous crimes. As a result, there is an undying need for cyber security, and therefore strong frameworks that will assist in combating botnet attacks. Hence, utilizing the frameworks specifically tailored for Bangladesh, will eventually result in reducing the risk of Bangladeshi government institutions and financial sectors being targeted by botnets. Consequently, lessening the economic damages to the country that come along with such atrocious attacks.

## 2.2 Life Cycle of Botnet

This section dives deep into understanding the complete life cycle of a botnet. Starting from its initial infection to its retirement, each of the parts will be covered thoroughly. In its first stage, the device becomes infected and transforms into a bot. Afterwards it is able to amplify the effect of the individual bot to a network of bots. This chapter also looks into the update and maintenance required to keep the network a continuous process. Along with that, the strategies of detection and mitigation avoidance are also explored. Lastly, this section also covers how a botnet is eventually sent to retirement.

### 2.2.1 Initial Infection

The first stage of the botnet life cycle is the initial infection and it's a crucial stage in the transmutation process. In this phase, a healthy computer or device turns into an infected device. Viruses or malicious software are being installed on the system without the awareness or knowledge of the user. These are installed onto the system

through which vulnerabilities or loopholes are discovered [8]. The main goal of this stage is to infect as many devices as possible to strengthen the botnet network. The methods used for initial infection can widely vary and can include [8]:

1. **Distribution of Malicious Emails:** Through social engineering techniques like attaching malicious links in emails, botnets are usually spread. The email containing the suspicious attachment leads the user to sites that look valid at first glance. These types of emails are distributed digitally for spear phishing in a large number.
2. **Software Vulnerabilities:** Botnets tend to make the most out of the vulnerabilities and the loopholes that exist in the software that are running or installed in the host's machine. For instance, a bot-infected host might be ahead of other vulnerable hosts in the search for other hosts with known vulnerabilities. Botnets exploit software vulnerabilities and security loopholes on host machines. A computer infected by a bot might be able to find other vulnerable machines more quickly. The LSASS vulnerability in Microsoft Windows is used quite often to spread and recruit more computers or devices into the botnet network.
3. **Instant Messaging:** Worms or bot binary are spread by using instant messaging platforms where the malicious links or files are sent to the General public pretending that they are from the contacts in the victim's list. Hence, the worms gain leverage from the trust of the victim since it shows that it's being sent from a known human to achieve its goal in infecting the victim.
4. **Peer-to-Peer (P2P) File Sharing Networks:** The bot binary replicates itself in the shared folders of the P2P file-sharing applications. It's done by creating really enticing file names to trick the other users into executing them.
5. **Secondary Injection:** Automated scripts are executed to run and install the bot malware, causing a healthy device to turn into a "zombie" or infected device.
6. **Use of Other Botnets:** There are some botnets that utilize already existing botnets for their distribution. They could occupy devices or systems that are already infected by older malware and haven't been resolved and update those devices with their own bot binary and hence through this method their network will extend.

### **2.2.2 C&C Establishment**

The next stage of the botnet life cycle is the C&C establishment. In this stage servers or other infrastructures are set up by the botmaster which acts as control points or central hubs from where commands can be issued to the bots that are infected and then extract data from them or execute malicious activities. To facilitate the coordination as well as the communication between the central command infrastructure that is controlled by the attacker and the compromised devices, command and control establishment is one of the central points in the life cycle of a botnet [18]. Principally, different malicious activities such as the launch of distributed denial-of-service attacks (DDoS), spam email dispersion, theft of sensitive information, and



more extensive spread of malware are controlled and enabled by this C&C infrastructure which gives the botnet operator full authorization over the entire network. The attacker is thus able to execute commands to groups of bots and individual bots through the encrypted C&C servers and make the bots download new and updated versions of the malware and commence specific malicious tasks.

**Decentralized Botnet Model:** Decentralized or P2P botnets do not have a single point of control [8]. The bots communicate directly with each other to share commands or instructions sent by the botmaster. As a result, the bots that are not centralized become more resilient when disrupted as there is no single server which can be targeted for the botnet take-down. P2P botnets are therefore harder to detect and dismantle.

**Centralized C&C Model:** In contrast, a centralized server or a group of servers is the control point from where commands are issued towards infected bots. Bot master or botnet compromised host usually sets up this server. The most famous protocols being used are IRC and HTTP. After the centralized C&C server or infrastructure is completely operational the botmaster gains unified control over the entire network which includes the infected bots. Consequently, the network then becomes a strong and powerful tool for cybersecurity breaches and other illegal activities [18].

The following are some of the most prominent command and control (C&C) establishment ways [18]:

1. **Single Star Topology:** A main C&C server is present and all the other bots are connected to it.
2. **Multi-server Star Topology:** The majority of the servers are used for redundancy and scalability. The bots connect to one of the several servers that are available.
3. **Hierarchical Topology:** Some bots are directly connected to the actual C&C server and are also connected to other bots they act as a middle bridge. This type of configuration is used to camouflage the actual C&C server.
4. **Distributed C&C Model:** The technique works as a peer-to-peer network in which every bot functions both as a client and a server. This type of model decreases the risk of the whole botnet being taken down in case of a single point failure.
5. **Communication Protocols:** Apart from IRC and HTTP advanced botnets may use encrypted P2P communications, which rely on protocols which are designed to ensure that there is a secure and private communication established between few people.

**C&C Communication Initiation:**

- (a) **Push Method:** Commands are being pushed from the C&C servers to the bots; this is an effective way of having instant action taken across the botnet.

- (b) Pull Method: Bots are stored in the cloud and periodically they check with the C&C to push the commands. This is a stealthier approach as it draws less attention and are harder to detect.

Figure 2.1 illustrates the phases of a botnet from initial infection to retirement.

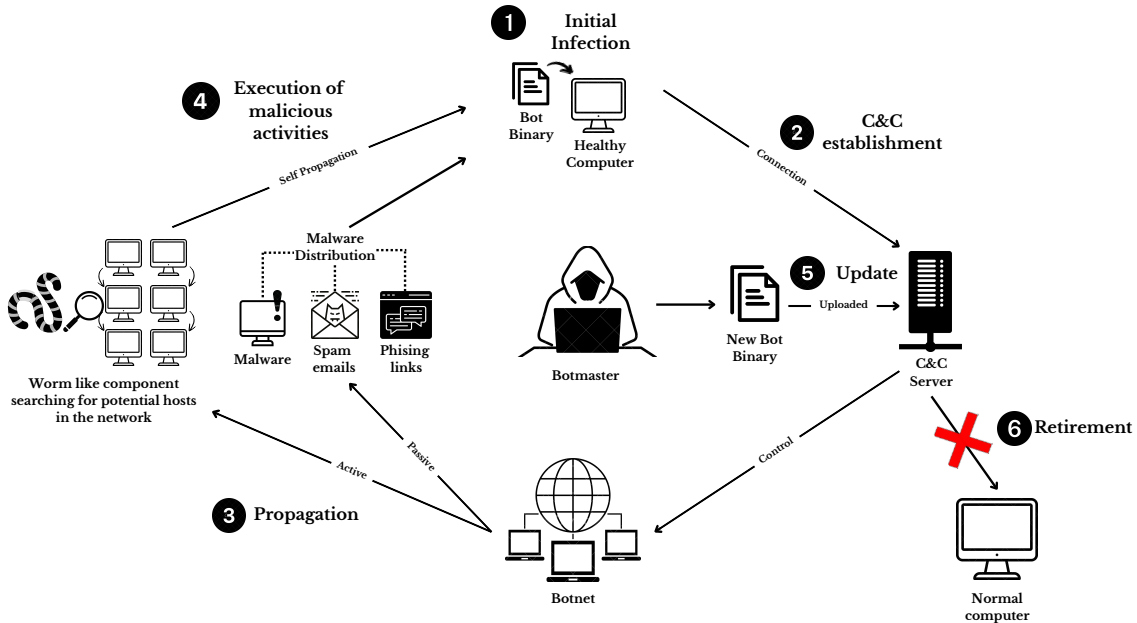


Figure 2.1: Life Cycle Of A Botnet

### 2.2.3 Propagation and Expansion

The spread of botnets occurs primarily through two propagation methods. They are active and passive.

**Active propagation:** Active propagation is autonomous and does not require any intervention by the user. The bot binary itself has autonomous scripts and can execute to scan potential hosts, identifying and exploiting known software vulnerabilities to infiltrate systems and incorporate them into the botnet network. For example, systems with common Windows vulnerabilities like LSASS, may be searched by a botnet which may employ advanced scanning algorithms. After identifying the vulnerabilities or loops they are then exploited by the bot binary which allows the botnets to propagate really efficiently and rapidly without the need of the bot master or any human intervention. These types of botnets are capable of replicating or cloning themselves and eventually create a massive network of infected devices [18]. Furthermore, some botnets utilize self-replicating malware's which are capable of spreading autonomously without direct human intervention. Through infective shared network drives and portable storage devices such as pen-drive or by taking advantage of loopholes in the network protocols, the malware variants propagate and expand more in scale.

**Passive Propagation:** Another form of propagation method is the passive propagation. In this form of propagation method some form of human intervention to an

extent is required for the propagation method to work. Social engineering techniques lure users into unknowingly help expand the botnet network, and this propagation method relies on the human vulnerability. For instance, links that lead to compromised websites or attachments that are malware-integrated gets spread through malicious emails. Social engineering tactics are used to mislead the receivers into clicking the links or attachments, sent via the emails. As a result, it downloads the bot binary and makes their system infected. As mentioned in the study [18], when the user clicks on the link, his/her machine gets infected, and the user is recruited into the team of a bot master without them even knowing about it. Moreover, botnets may compromise legitimate websites by injecting malicious code like SQL injection or exploiting vulnerabilities in web applications. Visitors to these compromised sites may unknowingly download the malware onto their devices or system and hence ultimately contributing to the botnet's growth.

## 2.2.4 Execution of Malicious Activities

After the systems of a victim gets infected through the botnet it is then connected to the network, it becomes one of the puppets of the network and is used by the botmaster for different malicious activities. According to the research [18], such activities can range from disruptive to absolutely heinous, which assists to represent the horizon of impact from botnets on cybersecurity.

1. Distributed denial-of-service (DDoS) attacks: DDoS is one of the most used strategies among the botmasters which aids in executing attacks more frequently. A large fleet of compromised devices are used and the botmaster overwhelm a target server with malicious traffic which ultimately leads to shutting the server down for legitimate users. Such attacks, as outlined in [18], are really hard to defend against due to the botnets distributed nature and the sheer volume of data it churns out overwhelming the systems capabilities.
2. Phishing Campaigns: A tactic where fraudulent emails or scam websites trick users into sharing sensitive credentials like passwords or financial details. Botnets excel at amplifying these campaigns so that it reaches more targets and boost their success rates, as discussed in [18].
3. Botnet-as-a-service: One of the most insidious platforms cybercriminals uses is botnet-as-a-service (BaaS). This makes it easy for botmasters, so they don't need coding expertise and can simply lease or purchase botnets to use for one's own personal criminal apparatus. From carrying out DDoS attacks to sending spam or distributing malware, as discussed in [8] BaaS is useful.
4. Crypto mining: Infected computers often contribute their processing power to secretly mine for cryptocurrencies like Bitcoin or Monero. Botmasters use these infected devices resources to earn a lot of mining cryptocurrencies as revealed in [18]. However, this activity comes at a cost for victims, making their system slow and rendering them useless to do any task and potentially hitting them in the wallet.

## 2.2.5 Maintenance and Updates

The maintenance and update of botnets are critical components that ensures their ongoing functionality, effectiveness, and patch the ability for the bot binary to evade any sort of detection. Regular updates following new cyber security feats are crucial for maintaining the operational integrity of the botnet and for circumnavigating emerging security defenses. These updates typically involve the botmaster sending commands to the compromised devices and using the C&C to instruct the bots to download and installed the updated binaries. These new versions of the malware may include modifications such as improved evasion techniques, performance optimizations, or bug fixes, in overall aimed at keeping the botnet undetectable and efficient [9]. In addition to software updates, botmasters frequently engage in server migration in case their C&C server is compromised or to move their server to a more advanced and undetectable host where the bots are transferred to a new C&C server. Server migration is crucial for maintaining the botnet’s stealth and operational continuity. By shifting the C&C servers, botmasters can avoid detection by security systems that may have identified and targeted the previous server [10].

From a financial perspective, the cost related to maintaining a botnet can vary significantly depending on the composition and usage. Botnets composed of Internet of Things (IoT) devices, such as security cameras or smart home appliances, are often more cost-effective to maintain due to the lower operational and management costs associated with these sorts of devices. Maintaining a botnet of desktop computers can be more resource-intensive but potentially more profitable when employed in a large-scale Distributed Denial of Service (DDoS) attacks. These attacks can generate substantial revenue by leveraging the botnet’s computational resources to disrupt services and force payments [3].

Moreover, botnet operators continuously innovate new strategies to adapt to security measures advances and as new vulnerabilities are patched. This includes developing new techniques for evading detection, enhancing the botnet’s resilience, and ensuring that the malware remains effective against updated security protocols [3]. The rapid pace of security updates demands an ongoing cycle of development and adaptation essential for the botnet’s sustained operation and success. Thus, the maintenance and updates of botnets are not just about keeping them functional but also about staying ahead of evolving security measures and maximizing their operational lifespan.

## 2.2.6 Detection and Mitigation Avoidance

Detection and mitigation avoidance is one of the most crucial aspects of the botnet life-cycle which ensures the botnet remains hidden and operational despite the defensive or security measures. It’s not a formal phase of the botnet life cycle but securing the bot from removal is essential for its longevity. The bot needs to consistently listen for commands from the Command and Control (C&C) Server, execute these commands, and send the results back to the C&C server, all while erasing evidence of its activity to stay undetected [11]. Various mechanisms are designed to hide the botnet and mask its components, such as C&C channels, bot masters, and bots. Widely used hiding techniques in botnets help to ensure these elements

remain difficult to discover [11]. Some of these techniques are:

1. **Ciphering:** Here, data or files are encrypted which makes it unreadable to the victim unless the right key is used to decrypt the data. In modern botnet models, C&C communications between the botnet and its servers are encrypted in order to make botnet analysis and identification difficult. This encryption method makes it practically impossible to establish efficient means of identifying the communication pattern and preventing C&C communication channels. For instance, Zeus and SpamThru Botnets implement encrypted channels.
2. **Polymorphism:** A technique where different versions of the source code of a program are created keeping the actual functionality being the same. This method constantly changes code to avoid detection. This variation in codes makes the signature-based detection process, which is used by most current antivirus tools, more challenging. Some notable botnets such as Zeus & Phatbot uses polymorphism.
3. **IP Spoofing:** It involves the sending of IP packets with fake source addresses and its commonly used in Dos attacks. This sort of method is used to evade IP filters and hide the origin of attack. This makes the true source of cyber criminals difficult to identify.
4. **Email spoofing:** This method works by sending emails with fake sender addresses or origin in the header. Commonly used in phishing attacks. It's used to trick receiver into clicking on malicious links or downloading malware by making them think the sender or origin of the email is legit. The links and websites they lead to seems legit but it's not and it's only a decoy of the legit website and they get the email, password or other credentials of the victim when they input those things in the website. It's made just to deceive people into thinking they are from a trusted source.
5. **Fast-flux Network:** A technique used to hide the true location of a final host on the network by using a large number of proxies (also known as flux agents) that continuously redirects user requests. These proxies change rapidly by using DNS entries with low TTL (Time to Live) making it difficult to trace.

## 2.2.7 Retirement

The retirement phase of a botnet marks the end of its active operation due to the decision of the botmaster because of external factors such as improved security measures or law enforcement intervention. This phase represents the natural conclusion of the botnet's life-cycle where the botnet either becomes obsolete, not profitable enough or is taken down by the botmaster voluntarily. Understanding the condition under which a botnet retires is crucial as it provides insight into the life-cycle's duration and the conditions which makes the botmaster decide to take it down.

Botnets typically retire for a variety of reasons, which may include:

- **Obsolescence Due to Security Improvements:** As botnets and malwares evolve everyday, so does its counterpart. As cybersecurity measures continue

to evolve many botnets become obsolete when there arrives security patches, improved detection systems or other measures taken by cybersecurity professionals. This leads to a significant reduction in the botnet's efficiency making it difficult for the botmaster to maintain their control over the infected devices. Once key vulnerabilities are patched and the botnet's ability to propagate is put to stop, the botnet may be obsolete as the infected devices are cleaned or isolated [21]. As a result the botmaster can no longer keep up with the security updates and eventually gives up.

- **Law Enforcement Intervention:** A significant number of botnets are dismantled by law enforcement agencies and they often collaborate with non-government cybersecurity agencies to put an end to botnet activities. Through coordinated efforts botnets are tracked and the C&C servers are seized or taken down causing the end of botnet activities. Well-known botnets such as the Mirai and Zeus networks were eventually dismantled by law enforcement actions that targeted their core operations [22]. As the number of unsupervised C&C servers and ISP's decrease, it gets hard for the botmasters to acquire the hardware required for botnet activities. And botmasters eventually take down their botnet due to this and for the risk of getting caught by law enforcement.
- **Voluntary Shutdown by the Botmaster:** In some cases, botmasters may voluntarily retire their botnets. This may occur for strategic reasons like to avoid detection by law enforcement or to prevent legal actions against them. In cases like this, the botmaster may remove the C&C server to avoid it getting tracked and issue command to the bots to make Voluntary retirement can also occur as botmasters scrap their old botnet, learn from the shortcomings and build more sophisticated botnet which may be more useful to them. [23].
- **Diminished Financial Returns:** When maintaining a botnet becomes financially unsustainable, botmasters may opt to retire the botnet. Factors such as the increased cost of hosting and maintaining C&C infrastructure, less profit from operations like DDoS attacks or even declining demand for botnet services can also make the botmaster abandon their botnets. The botnet-as-a-service (BaaS) model is sensitive to market fluctuations. When demand for these sorts of services drops, botmasters may retire their existing botnet operation and pursue a more profitable venture [24].

The retirement of a botnet, whether it being voluntary or involuntary does not always imply the complete end of botnet activities. Many botmasters abandon their obsolete botnet to develop or adapt to a more advanced botnet with improved evasion and propagation techniques. Additionally, the data and knowledge acquired from the old models can contribute to the creation of even more resilient botnets. Thus, botnet retirement is the end of a certain botnet's service or operation due to external factors like law enforcement, financial viability, and security advancements. [26].

The life-cycle of a prominent botnet known as Mirai Botnet has been shown in Figure 2.2. It surfaced in August 2016, and its initial infection was on 18th September, 2016. Since then the botnet grew at a rapid pace with more and more new C&C servers added. Large entities like OVH and the "Krebs on Security" website

fell victim of the Mirai Botnet. On 30th September, 2016 a pivotal moment in Mirai Botnet's life-cycle occurred when the source code of Mirai was publicly released allowing many attackers to replicate it and make variants of it [46]. Later on Mirai was used in several high-profile attacks and of them the most severe one was Dyn DNS attack which caused major service disruptions across internet. Then in early 2017, the author of the botnet was identified and was put under law and order. Hence, the author being arrested, initiates the retirement phase of the botnet [46].

## Mirai Botnet Timeline

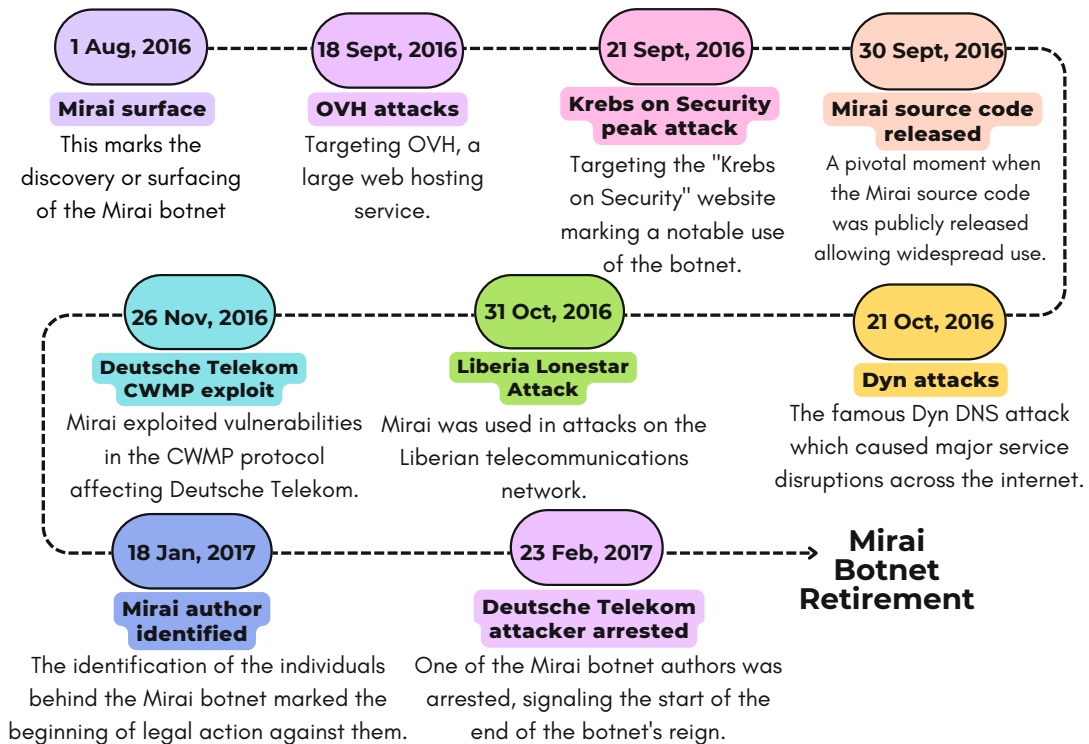


Figure 2.2: Mirai Botnet Timeline

In conclusion, this section explored the life cycle of botnets and its various stages in detail. Starting from the initial infection of the botnets which progresses through C&C establishment to its propagation, execution, and maintenance. It also covered how these bots can escape detection and mitigation strategies and their eventual retirement. During the initial phase, devices are often infected through malicious emails, exploiting software vulnerabilities or peer-to-peer networks. The botmaster aims to infect as many devices as possible to spread the botnet networks. Once infected, these devices are controlled by centralized C&C servers established by the attackers, using communication protocols like IRC and HTTP. The spread of botnets could occur either autonomously or through human manipulation, allowing the propagation of botnets to be more quick and efficient. Once established, botnets perform malicious activities like DDoS attacks, phishing campaigns, and cryptocurrency mining while often staying operational through ongoing maintenance and updates. Understanding these stages is crucial for addressing the botnet threat, especially given the sophisticated evasion techniques that keep botnets hidden from cybersecurity defenses. Techniques such as polymorphism, IP spoofing, and encrypted

communications help botnets avoid detection and prolong their operation, making mitigation efforts more challenging for cybersecurity professionals. By analyzing the entire botnet life cycle, this chapter emphasizes the complex and evolving nature of these cyber threats in modern cyberspace. Additionally, their ability to adapt to bypass security measures makes them a persistent challenge. Hence, grasping these stages and evasion strategies is crucial for continuous improvements in defense mechanisms against botnet attacks reducing their impact and securing digital environments.



# Chapter 3

## Literature Review

The comprehensive literature review encapsulates a broad spectrum of contemporary botnet research, encompassing critical topics like botnet life cycle, botnet business model, take-down attempts, dark web market, botmaster's perspective on conducting botnet attacks, and cybersecurity frameworks. All the studies provide evaluating methodologies, potential intensification, insights, as well as limitations. It provides an overview of the current cybersecurity environment and explains various topics such as the financial consequences of botnet attacks and industry-specific cybersecurity attacks.

This literature review articulates both strengths and limitations inherent in each study while recommending for future research.

The authors in [1] aspired to shed light on the development of cybercrime motivated through economic gains. They also informatively covered botnets working under an 'as-a-service' structure. The goal of this part was to look into the past of botnets, investigate previous take-down efforts, and find out the economic aspects of these darknet marketplaces. The authors utilized a handful of approaches by reviewing scholarly papers, surveys, and taxonomies on botnets to establish foundational knowledge. They employed business models like Alexander Osterwalder's Business Model Canvas and Michael Porter's Value Chain Model to analyze botnet elements as a business entity. The information laid out specified the economics of botnets and the techniques used to disrupt them by performing empirical research involving online databases and scholarly articles. The study also scrutinized 28 of the most appreciated operations conducted for the take-down of botnets from 2008 to 2021. It expanded on the importance of the particular financial construction in managing the botnet. The research also found that more awareness should be created concerning the economics of botnets and addressing the issues related to the take-down of the botnet. The study was to address the economic perspective as a way of creating new possibilities for destabilizing cybercriminal motivations. However, it overlooked some technical aspects like seizing down the "command and control" servers, that were previously the main focus during take-down attempts. This work could be improved further by concentrating on targeted approaches that disrupted income-generating parts of botnets, aiming to deter not only ongoing crimes but also discourage future cybercriminal activities.

In [2], authors focused on finding out the botnet's existence in the deep layers of the internet, then took it down, to pinpoint the virtual destination of dynamic DNS hosting, and finally the track down of the Mariposa botnet. Data like domains that were most commonly queried, were asked to be provided to the ones working on this shutdown of the botnet, from dynamic DNS providers. Consequently, they then changed the resolved IP of one of the C&C server domains to a sinkhole system they had created, with the help of DynDNS providers. Afterwards, the Mariposa botnet was successfully and completely shut down, and the owners Netkairo, Ostiator, and Jonyloleante were caught to have stolen data of more than 800,000 victims. Moreover, it was found out that after bribing an employee at the Spanish C&C domain hosting provider, the bot master had regained control of his C&C domain and then added new domains. As a result, the Mariposa bot's DDoS-ed Defintel's sinkhole was established. The attack was so strong that it took down the entire fibre provider's customer base. Although their strength was that they could make a fast recovery from it, they were attacked again the next day.

Putman et al. linked the details of the business model with botnets and the exploration of their owners' revenue streams were investigated in [3]. The purpose of the study was to investigate the dimensions and consequences of the botnets and estimate their costs at the organizational level by describing the stages and actors of a botnet's life-cycle. The authors reviewed many existing studies and scholarly papers, from which four distinct case studies were analyzed to gain insights into the revenue flows of botnets. It employed an equation from Charlie Miller's analysis and framework, Osterwalder Business Model Canvas, which shows how much an average malware developer earns and the maintenance cost of a botnet. Consequently, the study deduced that constructing a full-scale botnet from scratch is very costly while using a previously developed botnet comparatively requires minimal cost. The essential aspects of the botnet business model are the stages of the botnet life cycle, the actors involved, and the cost structure which were significantly highlighted in this study. Moreover, the inclusion of four more real cases also helped in creating a clear picture of the flows of revenues in botnets. However, the paper lacked an independent analysis of a range of economic consequences of botnet attacks on various institutions but rather relied on a collection of existing research papers and case studies. Therefore, for further improvement in this paper, future research is recommended to focus on preventing the revenue streams of botnets. With all the knowledge gathered regarding the botnets.

The authors in [4] explored the perspective of a botmaster and the complexities associated with arranging spam campaigns. They also provided a deep understanding of the underground economy of large-scale spam operations. This was done by inspecting a private forum called Spamdott.biz used by famous spam gangs. In this study, the researchers remarkably gained access to 16 servers used by Cutwail controllers. These servers had more than 2.35TB of data, spam templates and billions of targeted email addresses for spam campaigns. They even recovered detailed records for each spam bot stored in the databases. The database showed that in 2010, about 87.7 billion spam emails were mailed within a mere 26 days. The study underscored the statistics maintained by botmasters, the software used for bot and client management and the economic aspects of spam services. The direct access

to the actual command-and-control servers and a private forum used by notable criminal organizations showed the strength of this paper. The usage of a robust framework was also emphasized in the paper. However, the absence of a comparison with other similar botnets and a lack of explanation on the specific choice of the Cutwail botnet used acted as limitations. This paper could be improved further by certifying the data obtained from computer simulations based on certain parts of a botnet.

In [5], the authors focused on narrowing down insights from global cybersecurity frameworks. They also proposed a fully tailored Cybersecurity Policy Framework (CPF) for Bangladesh's financial sector. The task was to inspect COBIT 2019 and the European Central Banks Cyber Resilience Framework. This was done to find a more refined and customized solution for Bangladesh. The study extracted and included key concepts from distinguished frameworks such as COBIT 2019's 6 Core Principles, The European Central Bank's guidelines and the Federal Financial Institutions Examination Council's tools. An in-depth analysis of 16 papers including contributions by Akhter et al. (2021) showcased a wide range of novel approaches to guard from cyber threats. The study also included international perspectives after a thorough analysis of cybersecurity strategies. This paper conducted research and interviews with a diverse range of experts. These experts were from fields like bank CIOs, academics, policymakers and officials from Bangladesh Bank which added more depth and practicality to the research. The result was taken while focusing on crucial principles, governance risk management and collaboration of ideas from variable resources. The proposed Cybersecurity Policy Framework (CPF) had a precise goal of effectively reducing cyber risks, increasing awareness and promoting cooperation with the groups involved. Bangladesh's financial sector can approach cyber security with a robust plan by arranging global and local practices and combining them into a framework. Established frameworks, crucial insights from 16 papers and expert opinions from all fields are the strengths. The proposed CPF provides an extensive and detailed guide. This paper's weakness lied in getting validation from a hypothesis rather than collecting data from real-world observations. The research and proposed CPF offer a robust and solid foundation but adaptability due to the evolving nature of ransomware remains a challenge. Future research should focus more on the field-tested validation of the proposed CPF. It should also include numerical data from stakeholders from which its adaptability will rise. The CPF will continue to be a vital and robust solution to combat the evolving cyber threats in financial industries with constant revisions and the addition of new information obtained from the real world.

Hachem et al. covered the issues of botnets and its life cycle in [8]. Botnets are behind large-scale cyber-attacks such as spam campaigns, DDoS attacks, spreading malware and so on. The main goal of the research was to develop a clear understanding of botnets and their functionalities. Through this, the study aimed to combat botnets and detect them better. The life-cycle of the botnets was broken down into phases such as propagation, injection, control and attack. A significant contribution of this research was the creation of a detailed botnet classification system which helps to understand how they resist detection. Even though the paper focused mostly on the theoretical approach, the findings aligned with practical testing. For

future work, the research suggested delving deeper into botnet characteristics from the perspective of network providers to come up with more effective strategies for combating them.

The authors in [11] explained the analysis of botnets from a global perspective by focusing on the life-cycle stages. The researchers aimed to enhance the understanding of botnets by inspecting the most pivotal functionalities of the botnets. The study was conducted after reviewing literary papers on related works. The research contributed by highlighting the lack of uniformity in defining the stages of the life-cycle and it proposed a linear sequence of six stages; conception, recruitment, interaction, marketing, attack execution and lastly, attack success. The research further explained the importance of the marketing stage as it is crucial for improving prevention methods. Although the paper covered the life-cycle of the botnets extensively, it had limited discussion on the update mechanisms and mitigation strategies. For future work, the study proposed to work on the botmasters sell services.

The Tables 3.1-3.2 summarizes the research papers and reports that have been covered in this literature review, some of them have a few attributes in common with each other, while most do not. To differentiate this study from previous ones, the factors at focus are the Geo-location hub for these papers, whether they are specifically on botnets, the extent of coverage of economic aspects, thorough insights from multiple perspectives at once- attacker, general public, and security experts. Among the twelve papers listed, most of them include work that is related to botnets, some provide details on the economic impacts and aspects, none of them involves any research done on the public's outlook while only one paper contains data from the attacker's viewpoint, and a total of four papers comprise of details from security companies. However, none of the studies are a multiple perspective research, that is, all the angles have not been incorporated together in them. This is the gap that this study will be focusing on filling in. Consequently, two surveys have been carried out for the general mass and attackers, and an interview was taken of security professionals, to collect data and then analyze them. After analysis, the findings provide data-driven insights into the economic arena, as well as the impact and amount of usage of botnets that are specific to Bangladesh.

In conclusion, these researches underlined the importance of studying botnets and they illuminate the complex interplay between economic motivations and operational tactics. The proposed Cybersecurity Policy Framework for Bangladesh's financial sector exemplified the potential of integrating global insights with local context to forge appropriate defence strategies. The current collaboration and real-world authentication are essential to make sure that these frameworks effectively provide security. Deeper exploration into the life-cycle stages as well as botnet characteristics will enable us to intensify the capacity of cybersecurity workers to protect against cyber threats. Hence, securing our digital landscape for generations to come.

Paper Title	Author	Year	Geo-Location	Botnet	Economics Aspect	Attackers' Perspective	General Public's Perspective	Security Company Perspective
Botnet business models, take-down attempts, and the dark web market: a survey [1]	Georgoulas D. et al.	2023	Global	✓	✓	✗	✗	✓
Botnets: How to Fight the Ever-Growing Threat on a Technical Level [2]	Tiirmaa-Klaar H. et al.	2013	Global	✓	✗	✗	✗	✗
Business model of a botnet [3]	Putnam, C.G.J., et al.	2018	Global	✓	✓	✗	✗	✗
The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns [4]	Stone-Gross, B., et al.	2011	Global	✓	✓	✓	✗	✗
A Simplified Cybersecurity Policy Framework for the Financial Institutions in Bangladesh: A Survey of Literature [5]	Hasan, M.R.; Hossain, M.A.	2021	Bangladesh	✗	✓	✗	✗	✗

Table 3.1: Literature Review Summary (Part 1)

Paper Title	Author	Year	Geo-Location	Botnet	Economics Aspect	Attackers' Perspective	General Public's Perspective	Security Company Perspective
Bangladesh Cyber Threat Landscape 2022 [6]	Islam, M.S.; Alam, M.M.	2022	Bangladesh	✓	✓	✗	✗	✓
RBI Guidelines for Cyber Security Framework [7]	N/A	2016	Global	✗	✗	✗	✗	✓
Botnets: life-cycle and taxonomy [8]	Hachem, N. et al.	2011	Global	✓	✗	✗	✗	✗
Botnet: Evolution, life cycle, architecture and detection techniques [9]	Yadav, J.; Thakur, J.	2020	Global	✓	✗	✗	✗	✗
A survey of botnet and botnet detection methods [10]	Sonawane, S.	2018	Global	✓	✗	✗	✗	✗
Analysis of botnets through life-cycle [11]	Rodriguez-Gomez, R.A., et al.	2011	Global	✓	✗	✗	✗	✗
The deconstruction of the Mariposa botnet [12]	Sully, M.; Thompson, M.	2010	Global	✓	✗	✗	✗	✓

Table 3.2: Literature Review Summary (Part 2)

# Chapter 4

## Methodology

To gather empirical data, two distinct surveys and a semi-structured interview were conducted. The different targeting groups were the General Population, Attacker and Cybersecurity Professionals. To analyze the economic and online behaviors of the public and the motives of the attackers, data was collected from both groups. While surveying, it had been made sure that the test subjects' confidentiality would be maintained. So, both the attackers and the general public filled up the questionnaire while being anonymous. This aspect of confidentiality was present to protect privacy which often leads to honesty in responses, as a result enhanced data quality may be obtained. Maintaining privacy and inclusivity also helped in conserving ethical considerations of the data being collected. Lastly, a semi-structured interview with security experts had been held where one answer led to another spontaneous question. So, opinions and advice were obtained which provided great assistance in further analysis. This chapter is segregated into sections that dive into the intimate details of the surveys, how the gathered data has been analyzed, and what testing method was utilized for analysis.

### 4.1 Victim's Perspective Survey

This survey had been designed specially for the general mass who could be potential victims of botnet attacks carried out by cybersecurity attackers. The population characteristics in this case had been strictly set for Bangladeshi people. The form contained multiple sections that inquired about the respondents' census data, online behavior, awareness and security measures as well as practices and concerns regarding botnets. The survey form had been made anonymous which often directed participants to answer honestly. Consequently, it helped maintain the integrity of this research. Moving on, an astonishing figure of 605 responses were collected from participants spanning diverse demographics, including students, employed individuals, unemployed individuals, and retirees. Therefore, a comprehensive survey was conducted which included questions on:

- Demographics: Age, profession
- Internet Usage: Daily usage, primary device, type of connection
- Cybersecurity Awareness: Education, familiarity with botnets
- Experience with Cyber Threats: Incidents, behaviors related to cybersecurity

- Perceptions and Attitudes: Device security, willingness to pay for protection

The central focus of carrying out such a detailed survey was to uncover how the Bangladeshi people are suffering because of such malignant attacks. Moreover, it was possible to decode how aware they are about botnet attacks, what practices and steps they take to ensure safety against botnet threats, what their major concerns are, and whether it affects their online behavior. Thus, with this information along with other valuable data that are discussed in later chapters, it will be feasible to come up with solutions to combat malicious botnet attacks in Bangladesh's digital landscape.

## 4.2 Attacker's Perspective Survey

Data collection was carried out to obtain deep insights into the operational tactics, factors and influence of botnet attacks strategized by the cyber criminals. Indirect communication was made with attackers and hackers via a carefully crafted survey that indulged deep into their reasoning's, process of target selection, operational techniques, and their take on the relevant legal aspects. The data collection was done via the hacking community of Bangladesh through online communities of hackers, and several hacking forums, where the hacking forum's admins were handed the survey questionnaire and asked to forward them to the hackers. As a result, this micro-level task was primarily handled by the admins, and a total of 46 responses were acquired. As can be seen, the attacker response number is relatively small compared to the general public response figure (605). Yet, the attacker data is valid for analysis as local botmasters have been targeted which are only present in handful numbers and therefore, it is quite difficult to manage a huge number of responses. Therefore, the data's qualitative value is much higher which helps in revealing important trends and ultimately the bigger picture in this study. So, this data sample's uniqueness is strong as it gives out legitimate information that is otherwise not readily available anywhere for use. This survey covered:

- Cybersecurity Updates: Methods for staying informed
- Target Identification: Criteria for selecting targets
- Countermeasures: Encountered defenses and their impact
- Objectives and Monetization: Purposes of botnet deployment, revenue generation
- Operational Details: Compromise methods, propagation, C&C infrastructure, evasion techniques

The main goal behind this was to discover the impacts on the economic arena specifically within the context of Bangladesh's digital landscape because of these malicious activities. With the data collected from the survey, the operational complexities of botnet handling, the ever-growing techniques put in place by cybersecurity attackers, their effects on cybersecurity and thus, economic stability were explored. Therefore, this specific data collection acts as a vital source of knowledge which can be used to plan and develop specific strategies to reduce the influence of botnet attacks and



also reinforce preventive cybersecurity measures in Bangladesh and beyond.

### **4.3 Semi-structured Interview with Cybersecurity Professionals**

In a world where the usage of internet and devices are exponentially increasing, the threat of botnets and cyberattacks is significantly on the rise too. In recent times Bangladesh has been facing difficult challenges in defending their digital infrastructures. Pipeline Inc., a leading cyber defense company focuses on mitigating botnet activities, enhancing cybersecurity vulnerable sectors such as government, health-care, and financial, and raising awareness. A meeting was held with them to obtain professional insights into botnet management. It was not strictly structural, rather it was semi-structured. That means even though a set of questions were prepared beforehand, other unlisted questions were asked which arose due to the answers of previous queries. The discussion included:

- Botnet Spread and Propagation: Understanding mechanisms and trends
- Mitigation Strategies: Effective techniques and areas for improvement
- Challenges and Successes: Experiences in combating botnets and collaboration with legal authorities

Extended elaboration on this can be found in Chapter 7- Security Expert's Perspective.

### **4.4 Exploratory Data Analysis**

Exploratory data analysis (EDA) has been conducted on the gathered data from the general public survey and the attacker survey. The data analysis assists in understanding the data, identifying the distribution of variables, discovering anomalies, and formulating hypotheses like examining relationships between two variables. Additionally, it involves summarizing the data's main characteristics using descriptive statistics, visual methods like graphs, charts etc., and often includes strategies to handle missing data and outliers. Therefore, with the gained insights due to EDA, backing up hypotheses is possible. Those hypotheses can be tested to obtain additional information that can be used later when designing the cybersecurity framework. More elaborate discussion on data collection and exploratory data analysis can be found in Chapter 8 - Analysis & Discussion.

## 4.5 Hypothesis Testing

Hypothesis testing is a general statistical process that is used to draw conclusions on a population based on sample data. It involves making an initial assumption, which is the hypothesis, collecting and analyzing data, and then deciding whether to reject or accept the assumption. Essentially, it emanates whether the observed data is significantly different from what was expected or if it could have occurred by chance. There are five key components of hypothesis testing: the null hypothesis, alternative hypothesis, test statistic, significance level, and p-value. Among these, the null hypothesis is the initial assumption, usually representing no relationship between the variables. The alternative hypothesis is what needs to be proved—it often depicts an association between the variables.

Moreover, the test statistic is a numerical value calculated from the sample data, whereas the significance level is the threshold for determining whether the observed effect is statistically significant. Lastly, the p-value is the probability that the null hypothesis is true, so a p-value less than the significance level suggests rejecting the null value.

To analyze the relationships between the variables collected from the surveys, **chi-square hypothesis testing** was applied. The chi-square test of independence is suitable to determine associations between categorical variables. This research specifically uses the chi-square test because the survey data from the general mass and attackers are both categorical variables, making it the most appropriate testing method.

### Null and Alternative Hypothesis

For the chi-square test of independence, the hypotheses are typically formulated as: - **Null Hypothesis** ( $H_0$ ): There is no association between the two categorical variables. - **Alternative Hypothesis** ( $H_A$ ): There is an association between the two categorical variables.

### Test Statistic

The chi-square statistic is calculated using the following formula:

$$\chi^2 = \sum \frac{(O_i - E_i)^2}{E_i}$$

Where: -  $O_i$  is the observed frequency in the  $i$ -th cell of the contingency table. -  $E_i$  is the expected frequency in the  $i$ -th cell, calculated as:

$$E_i = \frac{\text{row total} \times \text{column total}}{\text{grand total}}$$

## Degrees of Freedom

The degrees of freedom ( $df$ ) for the chi-square test of independence is calculated using:

$$df = (r - 1)(c - 1)$$

Where:

- $r$  is the number of rows in the contingency table.
- $c$  is the number of columns in the contingency table.

## P-value and Significance Level

The calculated chi-square value ( $\chi^2$ ) is then compared with the critical value from the chi-square distribution table, based on the degrees of freedom and the chosen significance level ( $\alpha$ , typically 0.05). The p-value is calculated from the chi-square distribution, and if:

$$\text{p-value} < \alpha$$

Then the null hypothesis is rejected, indicating that there is a statistically significant association between the variables.

Moving on, hypothesis testing is used in different scenarios. In this research, chi-square hypothesis testing was applied to assess the relationships between the variables from both the general public and attackers' perspectives. The chi-square test is ideal here because it examines whether the observed frequencies in different categories deviate significantly from the expected frequencies under the assumption that there is no association between the variables. Further details of hypothesis testing are discussed in Chapter 5 and 6 - Victim's Perspective and Attacker's Perspective respectively.

Figure 4.1 illustrates the steps of methodology.

In conclusion, the reason behind picking each of these three subjects- the general mass, attackers, and cybersecurity professionals is that this study is focused on extracting full-proof information, for an effective cybersecurity framework design. That was why data had been collected from the public to decipher in what ways they may suffer, as well as from the attackers and their primary reasons for carrying out the botnet attacks. Finally, those expert opinions from the professionals assisted in easy linking of the dots between the insights gotten from the common people and the attackers. While conducting the surveys, ethical considerations like removal of biased data that produced skewed results, and maintaining privacy were prioritized. To name a few limitations that came along with this research are- lack of organized hacking platforms in the context of Bangladesh, leading to a lack of availability of local botmasters which resulted in acquiring a small sample for the attackers data. Although eventually, with the collected data it was possible to do exploratory data analysis, formulate hypotheses, then test the hypothesis using chi-square testing. To give an overview, all of these mentioned topics have been touched at a surface level within this entire chapter. Therefore, all the procured data paved the way

for a smooth crafting of a framework that will tailor the financial institutions' cybersecurity needs in Bangladesh. Meanwhile, reducing the economic damage to the country.

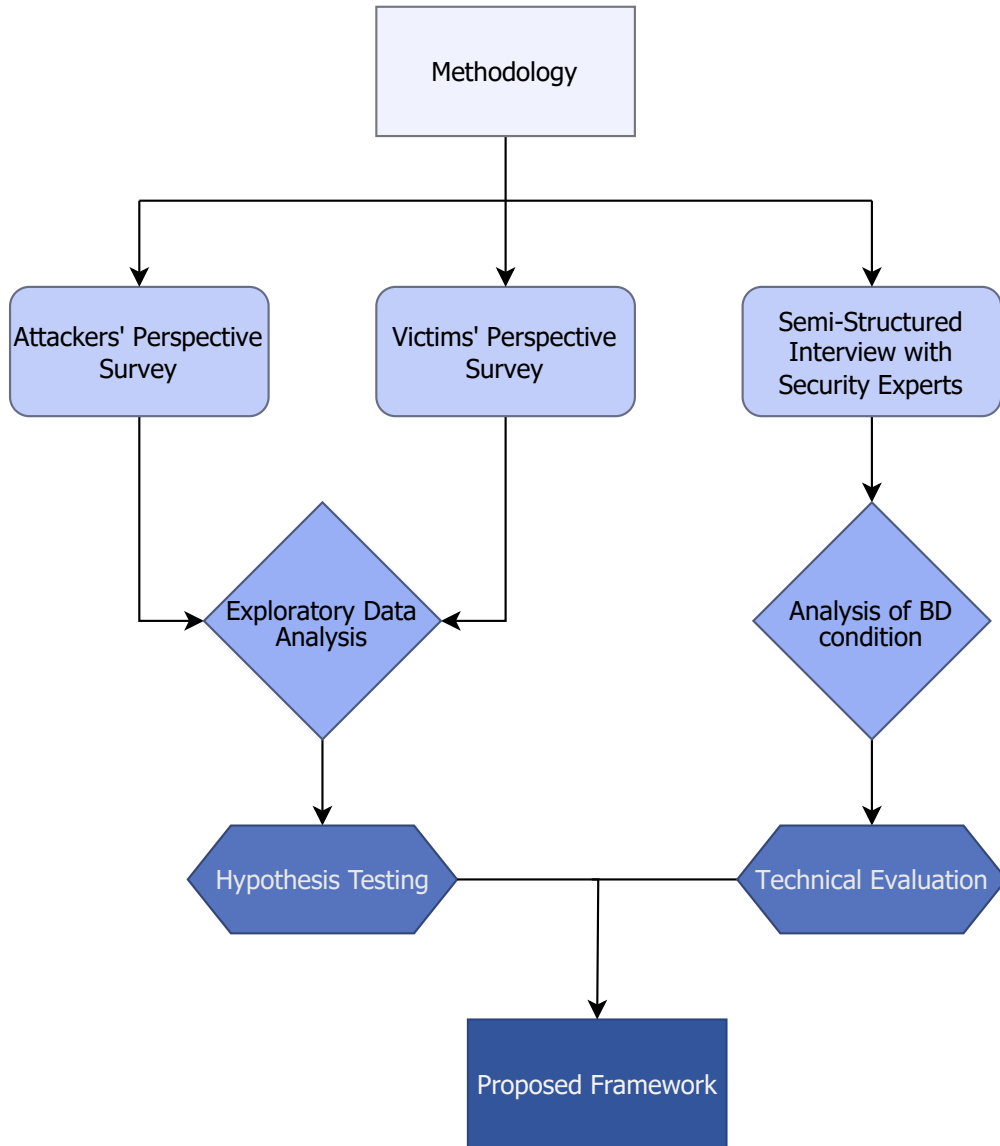


Figure 4.1: Methodology Flowchart

# Chapter 5

## Victim's Perspective

In this chapter, the study aims to shift the focus to the experiences and concerns of the general public's and potential victims of botnet attacks within Bangladesh. To gain an extensive understanding of the threat posed by botnets, a survey was designed with the general public's perspective in mind. The survey intended to explore their experiences, awareness levels, security measures, online practices, concerns, and behavior. From the data collected, the study will conduct a thorough analysis to capture these experiences, vulnerabilities, and insights crucial for developing effective and resilient countermeasures against botnet attacks. It will be ensured by following the Chi-square test of independence to analyse the associations of various variables.

Table 5.1: Demographics of Survey Respondents

Category	Attribute	Count	Percentage
Age	Under 18	13	2.1%
	18-24	521	86.1%
	25-34	39	6.4%
	35-44	4	0.7%
	45-54	18	3.0%
	55-64	10	1.7%
	65 or older	0	0%
Profession	Student	528	87.3%
	Employed	68	11.2%
	Unemployed	7	1.2%
	Retired	2	0.3%
Geo-location	Bangladesh	605	100%

From the demographics Table 5.1, the survey included 605 respondents from Bangladesh and participants were recruited through in-class distribution, and the survey form was shared with mutual contacts and were encouraged to disseminate it further to reach a broader audience. Participants for the victim's perspective were categorized by age, profession and geo-location. Additionally, respondents indicated their experience with botnet related threats and their familiarity with cybersecurity.

## 5.1 Data Analysis for Victim’s Perspective

In this section, the study will conduct exploratory data analysis on the survey data gathered from 605 respondents. The population characteristics in this study had been strictly set for Bangladeshi people. The analysis will focus on exploring the general public’s online behavior, awareness of botnets and security measures, and lastly, their practices and concerns. By examining these factors, the study aims to highlight the general public’s stance on botnets, including their ability to recognize patterns associated with these threats, their level of awareness regarding cybersecurity risks, and the actions they would take if they were to fall victim to such attacks. Ultimately, understanding these aspects is crucial, as these individuals represent potential victims of attackers and underscore the need for effective protective measures to safeguard their digital lives.

### 5.1.1 Demographics

The donut chart in Figure 5.1 illustrates the distribution of respondents who have experienced cybersecurity incidents, such as malware infections or phishing attacks. According to the chart, 36.03% of respondents have encountered such incidents, while 63.97% have not. This distribution highlights a notable portion of individuals who have faced cybersecurity challenges, emphasizing the need for increased awareness and proactive strategies to combat cybersecurity threats, as a significant segment of the population has already been impacted by such incidents.

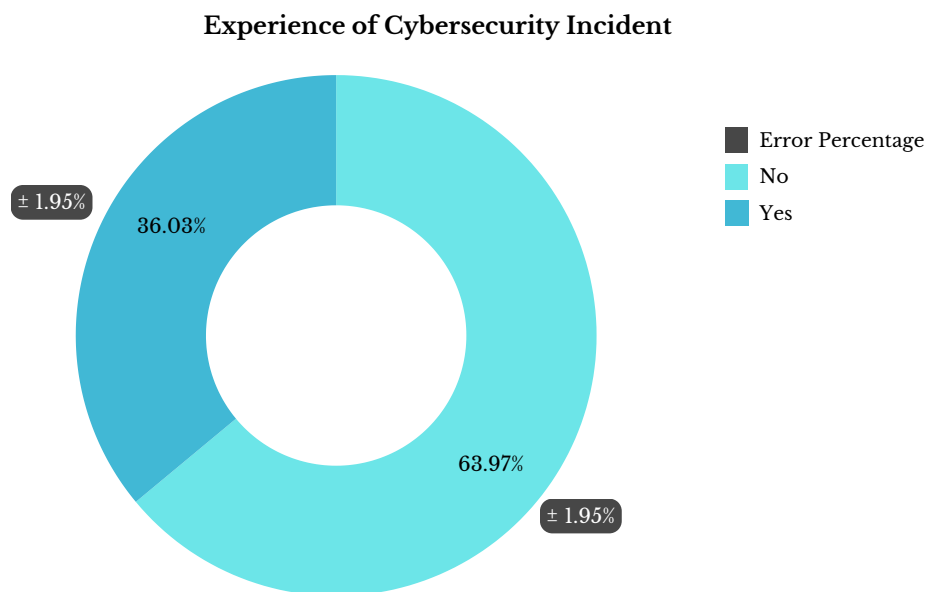


Figure 5.1: Experience of Cybersecurity Incidents

According to Kaspersky’s report [6], Bangladesh ranks 10th among countries and territories where users face the highest risk of online infections. During the reporting period, 20.81% of Kaspersky users in Bangladesh had their Web Anti-Virus triggered by Malware-class attacks. This statistic highlights the relatively high exposure to online threats in the country, where users frequently encounter malicious software, indicating a need for robust cybersecurity measures and awareness.

This horizontal bar chart in Figure 5.2 illustrates the distribution of respondents' familiarity with botnets. The different levels of familiarity are displayed on the y-axis, while the x-axis represents the number of respondents. Each bar corresponds to a specific familiarity level, with longer bars, indicating a greater number of respondents who fall under that category.

The chart shows that the largest group of respondents (409 respondents) falls into the "Not familiar" category, followed by those (163 respondents) who are somewhat familiar with botnets. A smaller portion of respondents (33 respondents) are very familiar with botnets, suggesting that although some are aware of the term, fewer have a deep understanding of what botnets are and the potential security risks they pose. This indicates a need for more education on cybersecurity threats like botnets as increasing familiarity with such threats could lead to better protection against them.

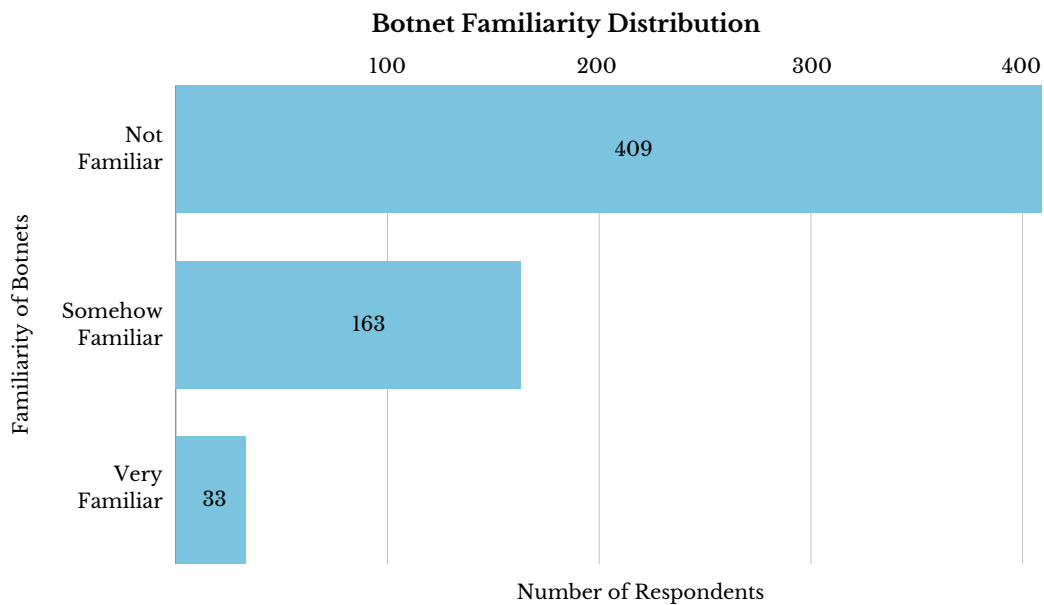


Figure 5.2: Botnet Familiarity

Bangladesh faces a significant risks of cyberattacks, largely due to limited familiarity with data protection and cybersecurity across the population. According to industry experts, this lack of awareness leaves individuals and organizations vulnerable to threats such as phishing, ransomware, and botnets.

A report from The Business Standard in 2023 [5] emphasized that while the number of internet users has surged, the corresponding increase in cybersecurity awareness and skilled manpower has not kept pace.

### 5.1.2 Online behavior

The pie chart in Figure 5.3 represents the distribution of responses to the question: “How much time do you spend on the internet each day?” Each slice of the pie corresponds to a specific time range, and its size shows the proportion of people who spend that amount of time online.

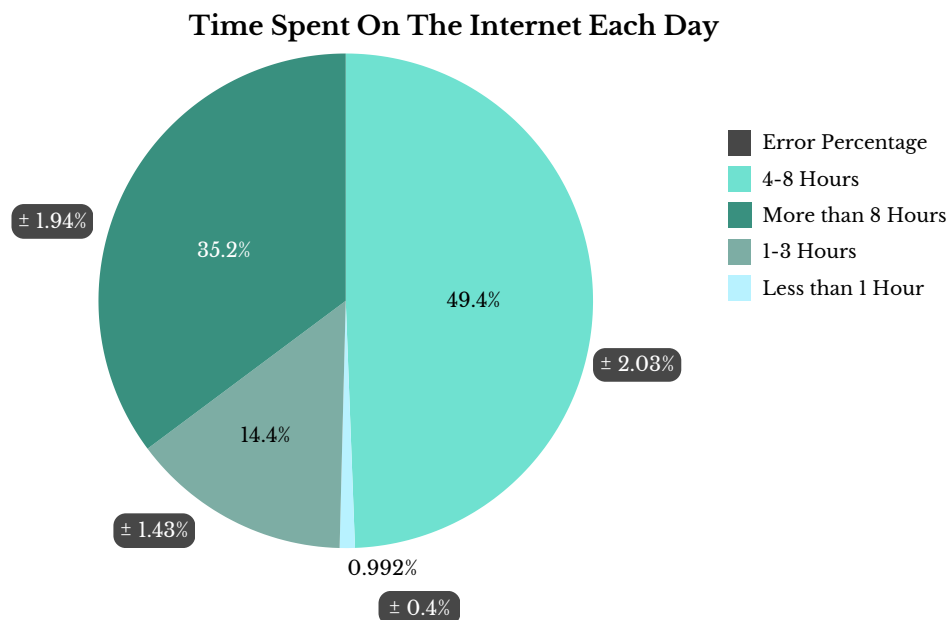


Figure 5.3: Distribution of Time Spent on the Internet Each Day

The chart reveals that about 50% of people spend between 4-8 hours on the internet daily, while 35.2% spend more than 8 hours online. In contrast, less than 1% of respondents spend under an hour on the internet each day. These figures highlight the significant role the internet plays in our daily lives, reflecting just how integral it has become to modern routines and activities. Moreover, it also suggests that individuals who spend more time online are more likely to face cybersecurity risks, as prolonged exposure increases vulnerability to various online threats.

The GlobalWebIndex report [4] indicates that on a typical day, internet users spend approximately 6.5 hours online. This reflects a significant portion of the day spent interacting with digital content and services, highlighting the critical role that the internet plays in our daily lives.

### 5.1.3 Cybersecurity Incidents by Device and Connection Type

In the survey of the general public, it is seen that out of 605 participants, the majority of people reported using smartphones as their primary device to access the internet. Figure 5.4 illustrates a sunburst chart representing the distribution of cybersecurity incidents categorized by device type, internet connection type, and incident status, providing a visual breakdown of how different factors contribute to the occurrence of cybersecurity issues. Specially, 46% used smartphones and 26% connected via home Wi-Fi, 12% of them have experienced cybersecurity incidents



such as malware infections or phishing attacks. And those using mobile data as their connection type, 6% experienced incidents, and 9% did not. Laptops were the second most common device with about 25% of the respondents, 19% connected to home Wi-Fi.

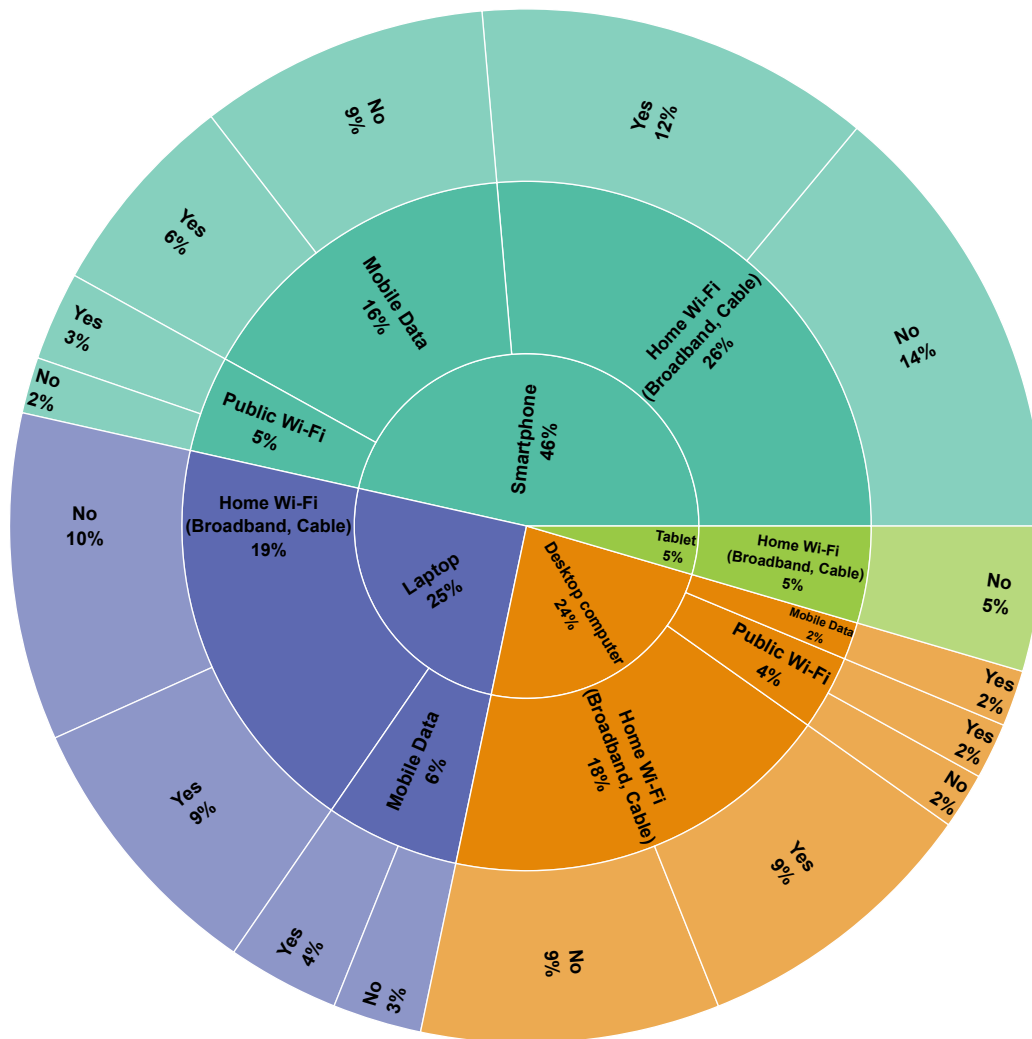


Figure 5.4: Cybersecurity Incidents by Device, Internet Connection Type and Incident Status (Log Scaled)

Among the laptop users on home Wi-Fi 9% reported similar incidents. For desktop computers which were used by 24% of the respondents. 18% of them were using Home Wi-Fi and 9% reported cybersecurity issues on home Wi-Fi. Public Wi-Fi saw minimal use and reported incidents across all device types. These findings from the sunburst chart reveals that smartphones connected to home Wi-Fi had the highest amount of reported incidents. This indicates the potential risks associated with this combination. Bangladesh witnessed 17.18% of mobile malware infections, placing

it among the top three countries with mobile devices infected by malware [62]. Furthermore, laptops and desktops show significant incidents rates when connected via home Wi-Fi, while mobile data and public Wi-Fi had fewer reported issues. The data shows the importance of security home networks, especially for smartphone users as they are more vulnerable to cybersecurity threats.

### 5.1.4 Awareness and Security Measures

Of 605 respondents, almost 79% of them did not receive any form of education related to cybersecurity, while the other 21% did. Figure 5.5 shows a clear correlation between cybersecurity education and familiarity with botnets. A significant 61.8% of respondents who did not receive education are unfamiliar with botnets, compared to only 5.79% of those who have received education. This highlights a major gap in awareness which suggests that individuals without cybersecurity education are more vulnerable to botnet-related attacks.

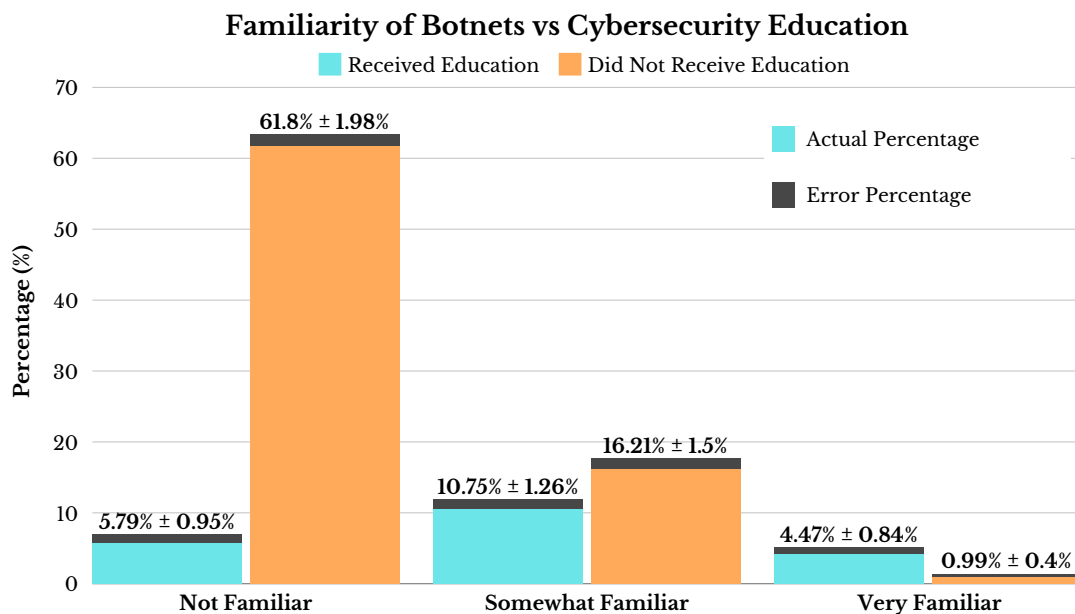


Figure 5.5: Familiarity with Botnets Based on Cybersecurity Education

People unfamiliar with these threats are more likely to fall victim to attacks such as Distributed Denial of Service (DDoS) or data theft through social engineering traps. The figure also demonstrates that only 0.99% of uneducated individuals are highly familiar with botnets, compared to 4.47% of educated individuals. This disparity underlines the critical importance of cybersecurity education in increasing awareness which will promote safer online behavior and empower individuals to respond effectively to cyber incidents and to protect themselves from being phished.

According to [36], education plays a pivotal role in reducing the likelihood of falling victim to cyber threats like botnets which further reinforces the importance of integrating cybersecurity awareness into educational curriculum or at least to include a cybersecurity training course for the employees in the financial sectors of the country.

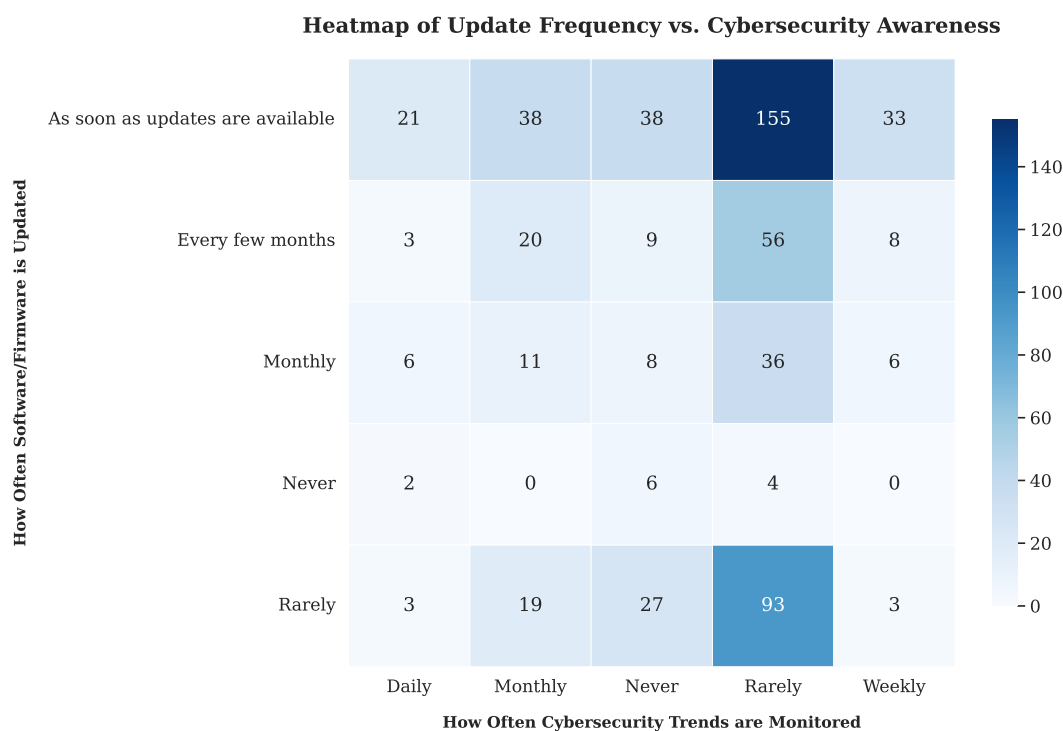


Figure 5.6: Heatmap of Update Frequency vs. Cybersecurity Awareness

Figure 5.6 reveals how often people update their software/firmware and how frequently they stay updated with cybersecurity trends. Out of 605 respondents, it is observed that a significant portion of 93 people rarely update their devices and also rarely monitor cybersecurity news. This puts them at high risk. Similarly, 56 respondents update every few months but still do not follow cybersecurity trends. On the other hand, only 21 respondents demonstrated ideal behavior by staying informed daily and updating their software promptly. Meanwhile, 155 people immediately update their devices but rarely check cybersecurity trends which suggests that many rely on automatic updates without being fully aware of potential threats.

The heatmap highlights that most people are either uninformed, careless with updates, or both, making it essential to raise awareness about cybersecurity risks. The goal is to ensure not just regular updates but also better engagement with cybersecurity news to minimize vulnerabilities.

### 5.1.5 Practices and Concerns

This grouped bar chart in Figure 5.7 visualizes the actions people take when they suspect their device is infected with malware, comparing those who have and haven't experienced a cybersecurity incident. The chart reveals that the majority of respondents, regardless of their experience, immediately run antivirus software upon suspicion of an infection. A substantial number also seek help from a professional when faced with potential malware. Interestingly, a small proportion of respondents ignore the issue even after experiencing a cybersecurity incident.

Moreover, there are still a few respondents who are unsure of how to handle the situation, regardless of their experience with cybersecurity incidents. This highlights a need for greater awareness and education on proper cybersecurity practices, regardless of past experiences.

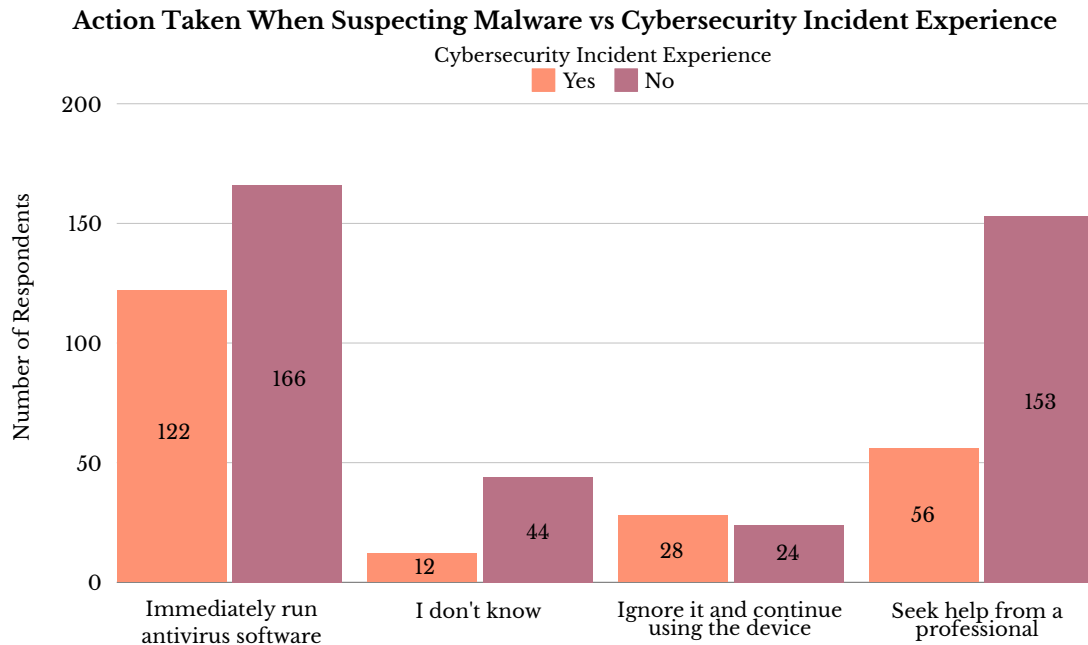


Figure 5.7: Action Taken When Malware is Suspected

In 2023, [2] Bangladesh experienced a significant increase in malware infection events, rising by approximately 71.39% compared to 2022. This surge is closely linked to the growing threat of ransomware, as many ransomware campaigns utilize malware like Trojan viruses to compromise systems. The sharp rise in these incidents highlights the growing cyber threat landscape in Bangladesh, particularly in high-risk sectors like banking and healthcare. This highlights the urgent need for stronger cybersecurity measures.

As individuals indulge in communication, e-commerce, and entertainment online, their trust in these online platforms and their concerns about security vulnerabilities are increasing due to their awareness of cyber risks. This analysis aims to explore the correlation between individuals' proactive information-seeking regarding cybersecurity and their perceptions of online trust and security concerns. Figure 5.8 illustrates the percentage distribution of fear of botnets in influencing trust in online platforms and e-commerce.

In a survey of 605 respondents, 75.6% of the individuals indicated that the fear of botnet attacks does in fact influence their trust in online platforms and e-commerce fields. And 24.4% of the individuals reported that such fear of botnet does not impact their trust in online platforms. From the survey result it is seen that a notable portion of respondents or consumers have crucial concern about trusting online platforms and e-commerce. The finding emphasises business and financial services to

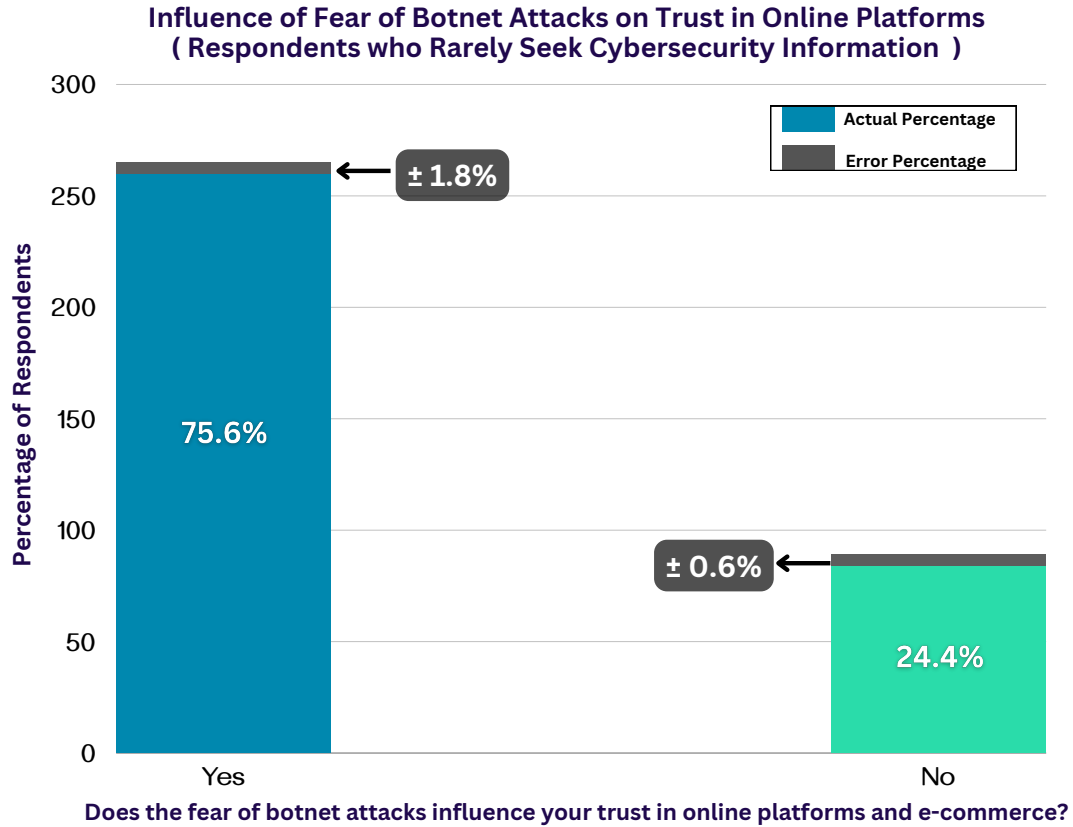


Figure 5.8: Influence of fear of botnet attacks

strengthen their cybersecurity and prioritise adapting a robust framework to reassure users and maintain their trust in online platforms and e-commerce. Preserving data consistency, trustworthiness, and accuracy throughout its life cycle is crucial, particularly for digital businesses vulnerable to attacks that can compromise data integrity [26].

## 5.2 Hypothesis Testing for Victim’s Perspective

In this section, the study aims to shift the focus to the experiences and concerns of the general public and potential victims of botnet attacks within Bangladesh. To gain an extensive understanding of the threat posed by botnets, a survey was designed with the general public’s perspective in mind. The survey was designed to explore their experiences, awareness levels, security measures, online practices, concerns, and behavior. From the data collected, the study will conduct a thorough analysis to capture these experiences, vulnerabilities, and insights which will be crucial for developing effective and resilient countermeasures against botnet attacks. This will be ensured by following the Chi-square test of independence to analyse the associations of various variables and to test the hypothesis that was formulated beforehand.

### 5.2.1 Experimental Design

For this study, a survey was designed for the general public and potential victims of botnet attacks. The demography was strictly set to Bangladesh and the survey contained multiple sections that inquired about the respondents' demographics, awareness and security measures, practices and concerns, and online behavior. The data was collected by visiting theory classes and mutual contacts where participants were briefed on botnets before completing the survey. Effectively, a staggering 605 responses were gathered. No personal identifiers or email accounts were recorded during data collection ensuring the privacy of the respondents. A detailed description of the survey design, participant selection, and statistical methods can be found in the Methodology chapter of this paper.

### 5.2.2 Study Objectives

The central focus of carrying out such a detailed survey was to uncover how the Bangladeshi people are suffering because of such malignant attacks. Hence, it was possible to decode how aware they are of botnet attacks, what practices and steps they take to ensure safety against botnet threats, what their major concerns are, and whether it affects their online behavior. Thus, with this information along with other sensitive data, it will be feasible to come up with a specific framework that will act as a shield against malicious cybersecurity attacks, that will not be limited to only the context of the digital landscape of Bangladesh.

### 5.2.3 Hypotheses

It is crucial to understand the perspectives of the general public and the potential targets of botnet attacks in order to develop a framework that will help protect them. Following that, this study formulated two hypotheses aimed at exploring the aspects of awareness, practices, and economic and online behavior of the respondents. Specifically:

- **Hypothesis 1:** Individuals who are aware of botnets and proactively update their software as a cybersecurity best practice have a higher willingness to spend money to stay protected against botnet attacks.
- **Hypothesis 2:** People who stay updated on various cybersecurity threats and best practices do not download illegally obtained cracked software or games.

### 5.2.4 Results and Analysis

In order to test the hypotheses, the chi-square test of independence was employed, which allows to statistically assess whether the observed relationships between these variables are significant or have occurred by chance. Since the data gathered are mostly categorical, the chi-square test of independence is ideal for determining the relationship between such variables. The following sections of this chapter will present the results of these tests and their implications for understanding the cybersecurity landscape in Bangladesh.

## Study 1: Awareness, Proactive Security Practices and Economic behavior

In this study, the relationship between an individual’s awareness of botnets, their proactive software updating practices, and their willingness to spend money to stay protected against botnet attacks will be explored.

The purpose of this study is to determine whether those who are more aware and proactive are indeed more inclined to invest in cybersecurity measures. In order to achieve this, the relationships among the variables ‘Awareness of Botnets’, ‘Updates Software’, and ‘Willingness to Spend Money’ needs to be investigated. This study will unveil correlations among the three-variables. It is crucial to understand if one being aware of botnets, leads them to practice digital hygiene, as well as, spend money to stay protected.

Table 5.2.1 presents the contingency table displaying the observed frequencies of individuals categorized by their awareness of botnets, their software updating behavior, and their willingness to spend money on cybersecurity. This table provides the foundational data for examining the potential relationships between these variables that will be further analyzed using the chi-square test of independence.

**Table 5.2.1: Contingency Table of ‘Awareness of Botnets’, ‘Updates Software’, and ‘Willingness to Spend Money’**

Aware of Botnets	Updates Software	Willingness to Spend Money		Column Total
		High	Low	
Yes	Proactive	31	60	91
	Less proactive	40	65	105
No	Proactive	40	154	194
	Less proactive	51	164	215
Row Total		162	443	605

Now, the null and alternate hypothesis for this study is to be formulated in order to determine if the variables are associated in the following manner:

**Null Hypothesis ( $H_0$ ):** Being aware and updating software proactively has no association with a higher willingness to spend money to stay protected against botnets.

**Alternate Hypothesis ( $H_A$ ):** Individuals who are aware of botnets and proactively update their software as a cybersecurity best practice have higher willingness to spend money to stay protected against botnet attacks.

To verify the null hypothesis, a significance level  $\alpha = 0.05$  will be considered. The three-variable contingency table will be taken into partial tables of two variables while keeping the third variable as a controlling factor. This will help determine whether the relationship of the two variables is independent of the third controlling factor. If the relationship between the two variables remains consistent across different levels of the controlling factor then it can be concluded that the three-variables are independent of each other. Now, the study will explore the relationship between awareness of botnets and software updates, with willingness to spend money as a

constant factor. Table 5.2.2 shows the observed frequencies for individuals based on their awareness of botnets and their behavior towards software updates.

**Table 5.2.2: Observed Frequencies for variables ‘Awareness of Botnets’ and ‘Updates Software’**

Awareness of Botnets \ Updates Software	Proactive	Less proactive	Column Total
Yes	91	105	196
No	194	215	409
Row Total	285	320	605

Using these observed frequencies, the expected frequencies were calculated. The expected frequencies are shown in Table 5.2.3 for the variables ‘Awareness of Botnets’ and ‘Updates Software’.

**Table 5.2.3: Expected Frequencies for variables ‘Awareness of Botnets’ and ‘Updates Software’**

Awareness of Botnets \ Updates Software	Proactive	Less proactive
Yes	92.33	103.67
No	192.67	216.33

The chi-square statistic is then calculated using the formula referenced in Chapter 3 of the Methodology:

$$\chi^2 = \sum \frac{(O - E)^2}{E} = 0.0536$$

Chi-square value,  $\chi^2 = 0.0536$

With 1 degree of freedom, the p-value is calculated to be 0.816, which is greater than the significance level of 0.05. Therefore, the study fails to reject the null hypothesis, indicating no significant association between awareness of botnets and proactive software updating behavior.

Similarly, the study investigates the relationship between awareness of botnets and willingness to spend money, while keeping software updates constant. Table 5.2.4 shows the observed frequencies for individuals based on their awareness of botnets and willingness to spend money to stay protected against botnet attacks.

Using these observed frequencies, the expected frequencies were calculated. The expected frequencies are shown in Table 5.2.5 for the variables ‘Awareness of Botnets’ and ‘Willingness to Spend Money’.

Chi-square value,  $\chi^2 = 13.1999$

With 1 degree of freedom, the p-value is calculated to be 0.00028, which is less than



**Table 5.2.4: Observed Frequencies for variables ‘Awareness of Botnets’ and ‘Willingness to Spend Money’**

Willingness to Spend Money \ Awareness of Botnets	High	Low	Column Total
Yes	71	125	196
No	91	318	409
Row Total	162	443	605

**Table 5.2.5: Expected Frequencies for variables ‘Awareness of Botnets’ and ‘Willingness to Spend Money’**

Willingness to Spend Money \ Awareness of Botnets	High	Low
Yes	52.48	143.52
No	109.52	299.5

the significance level of 0.05. Therefore, the study rejects the null hypothesis, indicating there is an association between being aware of botnets and having a higher willingness to spend money to stay protected against botnet attacks.

Lastly, the study investigates the relationship between updating software and willingness to spend money, while keeping awareness of botnets constant. Table 5.2.6 shows the observed frequencies for individuals based on their behavior towards software updates and willingness to spend money to stay protected against botnet attacks.

**Table 5.2.6: Observed Frequencies for variables ‘Updates Software’ and ‘Willingness to Spend Money’**

Willingness to Spend Money \ Updates Software	High	Low	Column Total
Proactive	71	214	285
Less proactive	91	229	320
Row Total	162	443	605

Using these observed frequencies, the expected frequencies were calculated. The expected frequencies are shown in Table 5.2.7 for the variables ‘Updates Software’ and ‘Willingness to Spend Money’.

Chi-square value,  $\chi^2 = 0.955$

With 1 degree of freedom, the p-value is calculated to be 0.3283, which is greater than the significance level of 0.05. Therefore, the study fails to reject the null hypothesis, indicating there is no association between proactively updating software and having a higher willingness to spend money to stay protected against botnet

**Table 5.2.7: Expected Frequencies for variables ‘Updates Software’ and ‘Willingness to Spend Money’**

Updates Software \ Willingness to Spend Money	High	Low
	Proactive	76.31
Less proactive	85.686	234.31

attacks.

**Result:**

1. Awareness of botnets & Updating software: No association
2. Awareness of botnets & Willingness to spend money: Association
3. Updating software & Willingness to spend money: No association

**Discussion:**

There is a significant association between awareness of botnets and the willingness to spend money on protection. However, no significant associations were found between awareness of botnets and updating software or between updating software and willingness to spend money.

One study highlights that individuals who are aware of cyber risks often prioritize financial investments in protective measures such as anti-virus software or tools that offer straightforward solutions, however, they are reluctant on consistently updating software [47]. The complexity of technical engagement of proactively updating software may not appeal to even those who are aware of botnets [47]. Therefore, this analysis suggests that although people who are aware of botnets are more willing to spend money on protection, having awareness of botnets does not make them more likely to update their software proactively.

**Study 2: Staying Informed on Cybersecurity Threats and Ethical Digital Behavior**

In this study, the relationship between an individual’s commitment to staying informed on cybersecurity threats and their likelihood of downloading illegal or cracked software will be explored. This study will help determine whether those who actively stay updated on cybersecurity issues are indeed less likely to engage in unethical digital behaviors such as using pirated software or games. Table 5.2.8 showcases the contingency table of observed frequencies of individuals categorized by their commitment to staying informed on cybersecurity threats and their likelihood of downloading illegal or cracked software. The null and alternate hypotheses for this study are as below:

**Null Hypothesis ( $H_0$ ):** There is no significant association between staying updated on cybersecurity threats and the likelihood of not downloading cracked software or games.

**Alternate Hypothesis ( $H_A$ ):** There is a significant association between staying updated on cybersecurity threats and the likelihood of not downloading cracked software or games.

**Table 5.2.8: Contingency Table of ‘Staying Informed’ and ‘Downloads Cracked Software’**

Staying Informed \ Downloads Cracked Software	Downloads Cracked Software			Column Total
	No, never	Yes, frequently	Yes, occasionally	
Daily	7	14	14	35
Weekly	11	10	29	50
Monthly	22	26	40	88
Rarely	117	79	148	344
Never	34	20	34	88
Row Total	191	149	265	605

Using these observed frequencies, the expected frequencies were calculated. The expected frequencies are shown in Table 5.2.9 for the variables ‘Staying Informed’ and ‘Downloads Cracked Software’

**Table 5.2.9: Expected Frequencies for variables ‘Staying Informed’ and ‘Downloads Cracked Software’**

Staying Informed \ Downloads Cracked Software	Downloads Cracked Software		
	No, never	Yes, frequently	Yes, occasionally
Daily	11.04	8.61	15.33
Weekly	15.78	12.31	21.90
Monthly	27.78	21.67	38.54
Rarely	108.60	84.72	150.67
Never	27.78	21.67	38.54

Chi-square value,  $\chi^2 = 14.40673$

With 8 degrees of freedom, the p-value is calculated to be 0.071, which is greater than the significance level of 0.05. Therefore, the study fails to reject the null hypothesis, indicating there is no association between staying updated on cybersecurity threats and the likelihood of not downloading cracked software or games.

**Result:**

- Staying Informed & Downloading Cracked Software: No association

**Discussion:**

The result of this study suggests that there is no statistically significant association between staying informed about cybersecurity threats and the likelihood of abstaining from downloading cracked software or games.

According to [48], individuals often rationalize risky behaviors believing that the consequences are unlikely to affect them directly. Furthermore, the desire to access expensive software or games for free often overrides an individual's awareness [48]. Therefore, the outcome of this study indicates that being knowledgeable about cybersecurity risks does not necessarily correlate with safer online behaviors such as avoiding illegal software downloads.

Therefore, this section unveiled and examined the experiences, online, and economic behaviors of the general mass of Bangladesh revolving botnet attacks. With the data collected from 605 respondents, the research uncovered valuable insights regarding the general public's awareness, security practices, and willingness to spend money in order to stay protected from botnet attacks. The findings of this section revealed that there is a significant association between the public's awareness of botnets and willingness to spend money on protection. However, this association does not reflect when it comes to proactively updating software. Moreover, the analysis of this chapter showed that staying informed about cybersecurity threats does not necessarily lead to safer online behaviors. As from this research it is seen that even though the general public were aware of botnets, they would actively download cracked software or video games. These insights underline the complexities of cybersecurity awareness and behavior which will help in formulating a well-suited framework for Bangladesh.

In conclusion, this chapter explored the perspectives of the general public in Bangladesh regarding botnet threats while focusing on their awareness, online behavior, security practices, and concerns. Based on data gathered from 605 respondents, valuable insights were uncovered about the population's familiarity with botnets, cybersecurity practices, and how these factors influence their response to potential threats. From the exploratory data analysis, it is revealed that a significant portion of the public lacks cybersecurity education which correlates with lower awareness of botnets and a greater vulnerability to cyber attacks.

Furthermore, while many respondents recognize the risks posed by botnets, there is a large majority of people who still do not actively seek information on cybersecurity trends or perform timely software updates. This highlights the need for more comprehensive cybersecurity awareness programs and practical measures to protect the public from evolving cyber threats. This also explains why most people have reported not experiencing any cybersecurity incident as most are not educated or aware about this topic. It is also discovered that most mobile users face security incidents compared to laptop or desktop users highlighting the importance of security home networks. Moreover, the analysis demonstrates that concerns about

botnet attacks have a notable impact on trust in online platforms and e-commerce which further emphasizes the need for robust security frameworks in Bangladesh. From the hypothesis testing, the findings reveal that there is a significant association between the public's awareness of botnets and willingness to spend money on protection, however this association does not reflect when it comes to proactively updating software. Furthermore, the research explored that staying informed about cybersecurity threats does not necessarily lead to safer online behavior. These insights provide critical input for shaping future strategies and protective measures to safeguard individuals against botnet attacks.

# Chapter 6

## Attacker's Perspective

In this chapter, the aim is to explore the mindset of cybercriminals, specifically those who orchestrate botnet attacks. To develop a robust defence against botnet attacks, it is crucial to gain insight into the attacker's perspective on their motivation, their strategies and their operational tactics. To achieve that, a detailed anonymous survey was conducted among botmasters in Bangladesh, focusing on their strategies for target selection, operational techniques and views on legal risks. By analyzing these responses, this study aims to uncover the driving factors behind these cybercriminal's activities and the impact of their actions on the broader cybersecurity landscape. Therefore, understanding the attacker's perspective will not only be essential for predicting future threats but also for developing policies and strategies that can protect the digital infrastructure of Bangladesh. In the following sections of this chapter, the Chi-Square test of independence will be applied to determine any association present in the variables and test the hypotheses this study formulated beforehand. Additionally, exploratory data analysis will help visualize trends in operational techniques and strategies among botmasters, providing deeper insights into their behavior.

### 6.1 Data Analysis for Attacker's Perspective

This section delves into the insights gathered from attackers' perspectives regarding the deployment and use of botnets using the data collected from the survey. The analysis focuses on several key aspects, such as the attackers' primary goals, methods of information gathering, financial considerations, and the operational techniques they employ. By understanding these factors, the research aims to shed light on the motives and strategies used by attackers in targeting vulnerable systems. Each subsection explores these dimensions in detail, providing a comprehensive overview of how attackers adapt their techniques to maximize the effectiveness of botnet attacks.

**Limitations:** It is important to note that the survey conducted for the attacker's was fully anonymous and no personal information or demographic information such as age, gender or education level was collected. This limitation was implemented to ensure the anonymity of the respondents.

### 6.1.1 Attackers on Goals & Target Selection

Based on the data gathered from the survey conducted among local attackers in Bangladesh, it was observed that India is the primary target for botnet attacks, followed by Bangladesh and Pakistan. Interestingly, neighboring countries such as Nepal, Bhutan, Afghanistan, Sri Lanka, and the Maldives appear to avoid being targeted by local botmasters altogether. This trend seems to be closely tied to the population size of each country. The larger the population, the higher the potential success rate of botnet attacks. Figure 6.1 illustrates the distribution of botnet attacks in South Asia, highlighting the countries targeted by local attackers in Bangladesh.

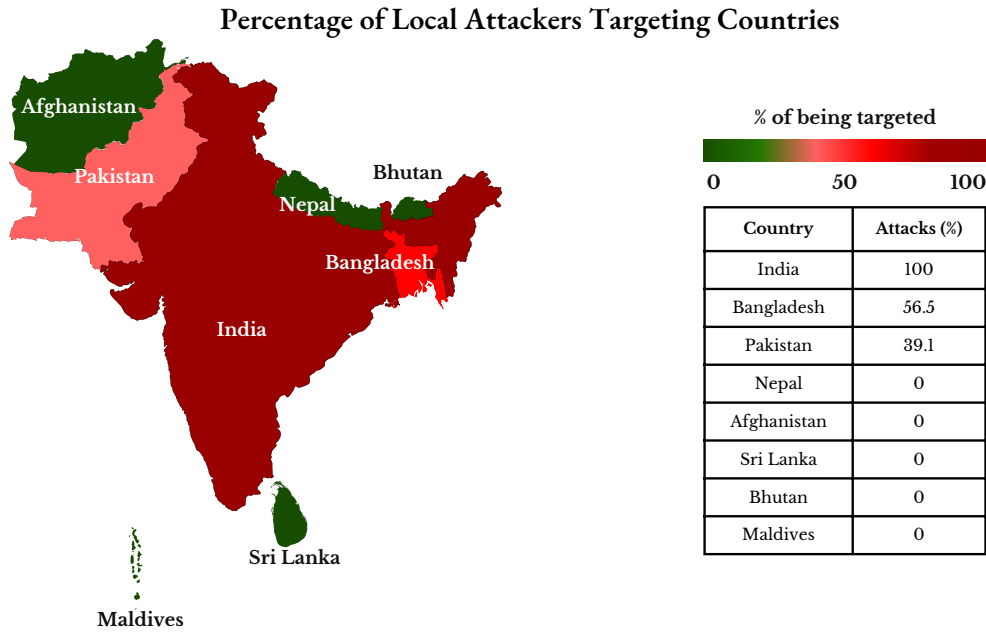


Figure 6.1: Botnet Attack Distribution in South Asia

It is notable that India faced over 500 million cyberattacks during the first quarter of 2023 [13]. This had contributed to a significant amount of the global total. Since in South Asia the top 3 countries in terms of having a large population are India, Pakistan and Bangladesh respectively, it confirms the assumption that attackers prefer to target largely populated countries. Bangladesh faces 56.5% of the botnet attacks in South Asia according to survey findings. This indicates that there are vulnerabilities in Bangladesh’s cyber defences due to sudden advancement in technology and lack of awareness about cyber threats. Pakistan is likely to be targeted 39.1% of the time according to the data gathered. Meanwhile, countries with relatively smaller population are left untouched by the local attackers. This signifies that countries with smaller population are of limited economic value to the local botmasters.

Understanding the targets of cyber attackers is essential for disrupting their financial motives. From the survey data, it can be seen that there is a clear hierarchy of vulnerability. The government institutions and small scale businesses are targeted the most for botnet inclusion. Meanwhile, large corporations are least targeted. This inconsistency highlights that attackers find it easier to breach government and small

business networks likely due to their lack of cybersecurity knowledge and weaker defence mechanisms. On the other hand, large corporations care about their data and security which is why they have stronger walls to protect them from such attacks. Figure 6.2 illustrates the percentage of targets for botnet inclusion. It is observed that 60.9% of the time, botmasters target government institutions for inclusion whereas about 32.6% of the time targeting large corporations.

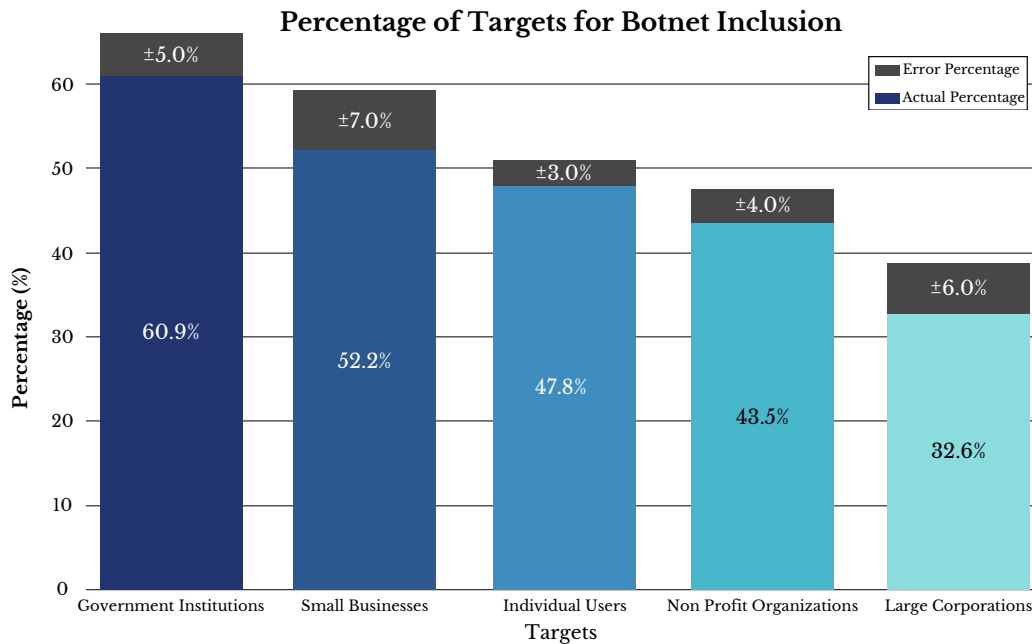


Figure 6.2: Targeted Entities for Botnet Inclusion

Bangladesh faces advanced cyber threats such as ransomware attacks on government agencies and businesses in 2022, with hackers demanding cryptocurrency payments, and an increase in phishing scams targeting online consumers with fake emails or SMS. These threats highlight the urgent need to enhance cyber defenses, incident response, and security awareness across the nation [63]. According to [14], the government institutions often possess limited cybersecurity resources compared to big corporations which creates a gap to defend against cyber threats. The government emphasizes more on national security rather than economic risk which may hinder their ability to address cyber threats effectively. The report [14] further adds that collaboration between government and the private sector are necessary to combat the cyber threats in the country. With both private sectors working with the government, the country can easily tackle any sort of cyber attack.

Botnets are utilized by attackers for multiple purposes such as launching DDoS attacks or conducting phishing campaigns. From the survey findings, it is observed that the local attackers mostly intend to use botnets to launch Trojan attacks as their primary goal. In order to achieve this, they rely on social engineering tactics to propagate their network. Figure 6.3 illustrates the percentage distribution of primary goals for launching botnet attacks. It is noticeable that 78.3% of the attackers use botnets to launch Trojan attacks, followed by 34.8% using them for cryptocurrency mining. 28.3% of the attackers are commencing DDoS attacks, 17.4%



distribute spam emails, and lastly, 8.7% of the local botmasters' primary goal is to ex-filtrate data through botnets. These findings highlight the diverse motivations behind botnet deployment in the local context. Understanding these goals can help in developing targeted countermeasures against these threats. Moreover, the botmasters rely on social engineering which emphasizes the need for increased public awareness and education regarding cybersecurity.

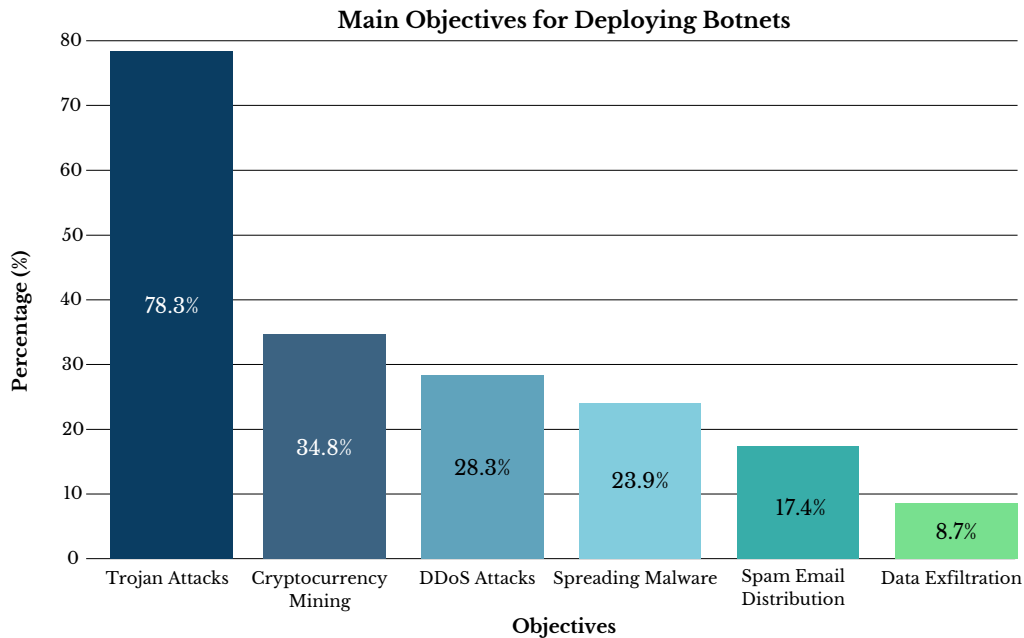


Figure 6.3: Distribution of Primary Goals For Launching Botnet Attacks

According to [15], social engineering remains the most used tactic among the cybercriminals. Even though it is detectable, general public's still fall prey to these tactics by being easily deceived. By offering lucrative deals or offers, the attackers hide malicious content that can collect victims' sensitive data. These stolen data are then sold in underground markets. Additionally, The Big Data provides attacks with the means to exploit datasets for commercial ventures by letting them sell stolen data [15].

Figure 6.4 illustrates the propagation tactics used by local botmasters who launch Trojan attacks as their primary goal of using botnets. It is observed from the data collected that about 52.8% of the botmasters rely on social engineering tactics and phishing as assumed earlier. 19.4% of the botmasters propagate their network through compromised devices and 11.1% of them rely on self-propagation.

A small fraction of the botmasters use sophisticated tactics. Among which, 8.3% of them take advantage of unpatched software to infiltrate, 5.6% of them abuse network vulnerabilities, and lastly 2.8% use remote access tools to expand their network of bots. Therefore, it is notable that more than half of the botmasters commencing Trojan attacks opt for social engineering tactics.

This highlights the vulnerability of the general public to social engineering tactics. Many users, due to a lack of awareness or proper cybersecurity education,

are easily manipulated into clicking malicious links. This allows botmasters to gain unauthorized access to their systems which allows them to exploit the users' limited understanding of potential online threats.

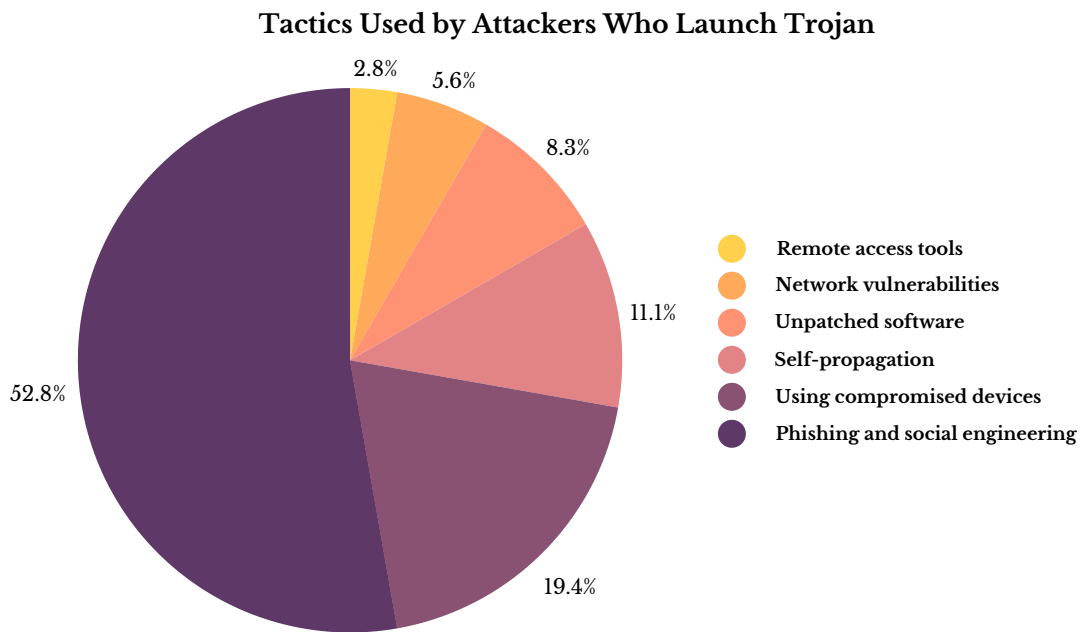


Figure 6.4: Propagation Tactics Used By Attackers Who Launch Trojan Attacks

### 6.1.2 Attackers on Information Gathering

The sources of information that attackers gather and the level of interest of the attackers in getting updated with the latest trends can be analyzed and various conclusions can be made about the potential attack scenarios. Awareness of these aspects lead to proactive approach in preventing cyber threats. Upon examining the survey data, it is observed as seen in Figure 6.5 that most attackers (76.1%) do not rely on staying updated with cybersecurity trends. This means that their methods are simpler and less prone to change as they rely on basic strategies which do not need regular updates due to emerging cybersecurity measures.

It has been projected that they are likely to employ conventional and possibly obsolete techniques that still work because of the weak cybersecurity in Bangladesh. Strengthening defenses against well-known attack vectors could mitigate many threats posed by this majority. Meanwhile 23.9% of cyber attackers gather information on cybersecurity trends indicating that the more advanced attackers having knowledge of security measures are capable of avoiding detection and even tackling them. It is in the same light that these attackers may prove to be more effective in cracking the current trends in security. To counter these more sophisticated 23.9% of the attackers, it's crucial to implement advanced detection and prevention mechanisms that are capable of handling evolving threats.

### Proportion of Attackers Gathering Info on Cybersecurity Trends

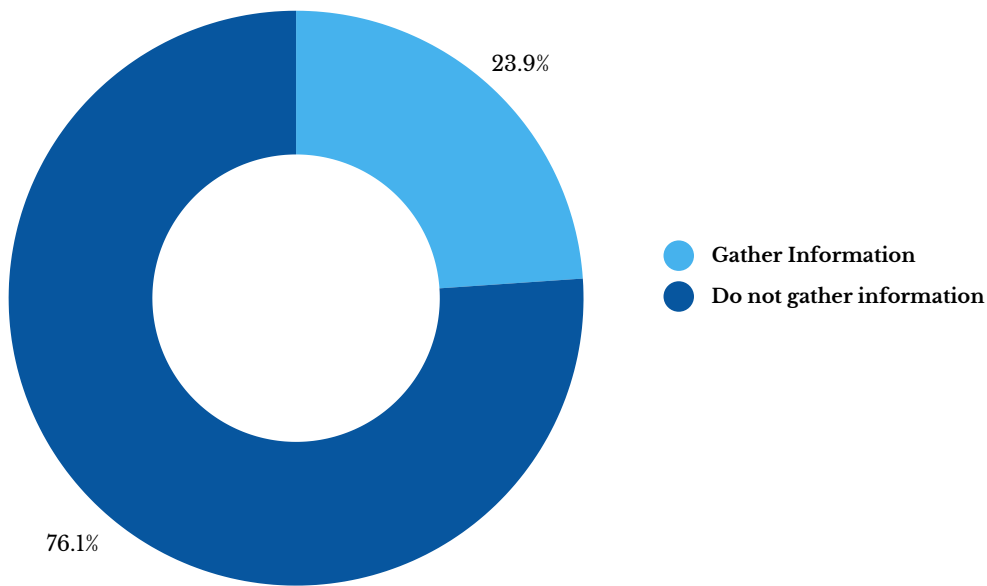


Figure 6.5: Proportion of Attackers Gathering Info on Cybersecurity Trends

Investigating the day-to-day activities of the minority that comprises local attackers who are into researching the trends in cybersecurity offers vital insights on how they operate. As a result of careful analysis, it can be noted that such people mostly tend to turn to a number of resources in order to be updated. Foremost among these sources are incident reports and case studies, which serve as practical learning tools, offering firsthand accounts of security breaches and their implications. Additionally, a significant number of attackers monitor security conferences and webinars, recognizing the value of real-time updates and expert insights shared in these forums.

In addition, a less numerous but still significant part of the malicious activity can be characterized by a focus on academic papers and research articles as sources of detailed information and expert views on the newly emerged threats on the cybersecurity scene. Figure 6.6 illustrates the distribution of information sources for the local attackers who gather information to stay updated on cybersecurity trends. It is observed that about 5.4% of attackers participate in red team exercises and take advantage of the information and experience that they gather.

Furthermore, some of them indeed engage with cybersecurity experts and follow them on social media sites, where the experts provide carefully filtered content along with their opinions. This approach of sourcing information is another indication of a strategic planning approach that these attackers possess, thus making it difficult to anticipate and counter their actions. As pointed out in [6], most institutions in Bangladesh are reluctant to report any forms of cyber attack to the public since this may lead to victim blaming which is why only 19% of the institutions that were interviewed disclosed that they had ever been victims of a cyber attack. Therefore, the incident reports which these attackers are relying on are more likely to be incident reports originating from another country and not Bangladesh.

### Distribution of Information Sources for Local Attackers

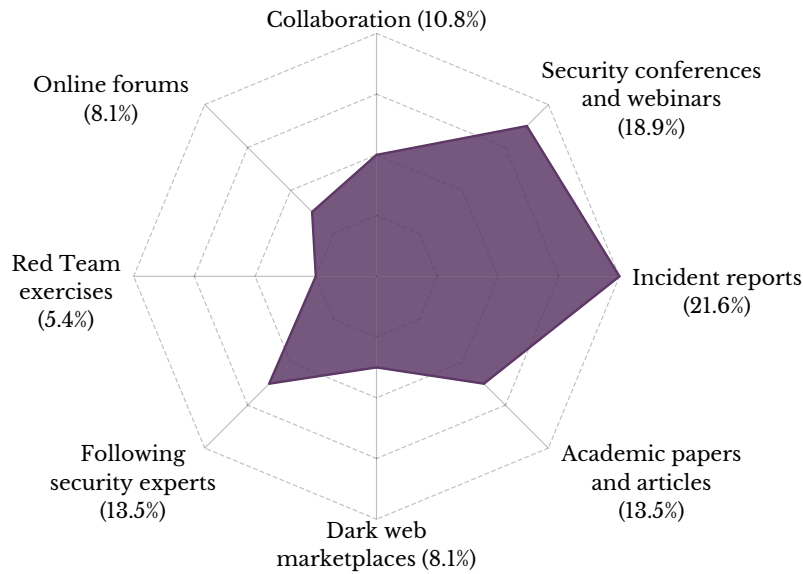


Figure 6.6: Information Sources for Local Botmasters

### 6.1.3 Financial Aspects

Approximately 52.2% of the attackers leverage off of stolen data and financial information as their primary source of income. The stolen information are likely to be sold on the black market. This indicates that data breaches and financial frauds bring in the most lucrative rewards for these botmasters. Figure 6.7 demonstrates the distribution of primary sources of monetization for local botmasters. It is observed that about 10.9% of the attackers rent out their botnet for DDoS attacks, 8.7% of them monetize through spreading ransomware, distributing spam emails and phishing links, and through click frauds. This not only highlights that the botmasters are leveraging off of general public's lack of awareness but also the diverse forms of services they can monetize from. 6.5% of the botmasters provide botnet services and another small portion of the attackers sell access to compromised devices. This underscores the growing market for botnet-related services which is directly contributing to the scalability and persistence of these networks.

Furthermore, it is worth mentioning that all 46 respondents have chosen cryptocurrencies as their choice of transactions for these illicit activities, which highlights that they prefer this digital form of transaction for anonymity and flexibility. According to [35] Crypto transactions are prohibited in Bangladesh because it violates the Foreign Exchange Regulation Act 1947 and the Money Laundering Prevention Act 2012. Yet, from this analysis, it is discovered that the local botmasters partake in Crypto transactions which shows a serious lack of enforcement and suggests that stronger actions are needed to stop illegal financial transactions in the country.

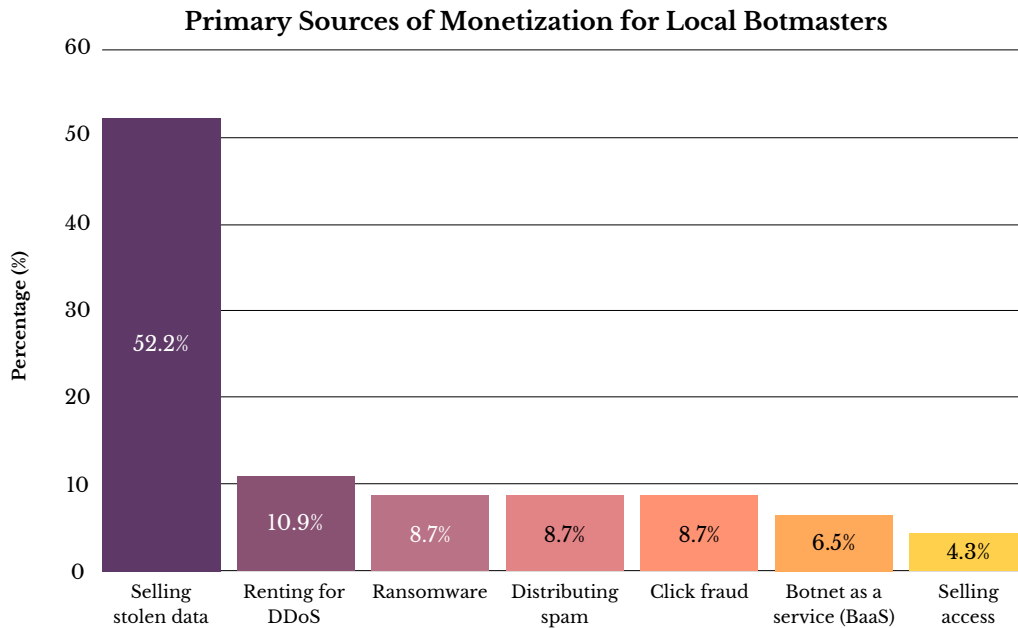


Figure 6.7: Primary Monetization from Botnet Attacks

Figure 6.8 reveals the monthly income range in BDT from selling stolen data by attackers. Among the attackers who sell stolen data, 66.7% earn about 50,000-100,000 BDT and about 8.3% of them have responded to earning more than 100,000 BDT per month. This aligns with the study findings as attackers tend to target government institutions more than any other entities. Stolen data, such as financial or personal information are of significant value in the cyber crime world. Demand for such data, driven by identity theft, fraud and other criminal pursuits influences its price ranges [16]

66.7% of attackers chose to estimate a monthly income of 50k to 100k by selling stolen data. This range indicates that a moderate level of profit and also that they possess relatively valuable data. However, this estimate has a margin error of 9.6% indicating variations in actual earning due to factors like data quality and demand in market. While 16.7% attackers chose 10k to 50k BDT as they may be dealing with less valuable data which could be outdated credentials or less sensitive [16]. There is a margin error of about 7.6%. And 8.3% attackers are more likely to have access to lucrative data sets or credentials of high-value individuals or organizations. This income range has a margin of error of 5.6% which suggests a relatively consistent income within this range. Lastly, 8.3% of attackers report monthly income range of more than 100,000 BDT per month. This huge number indicates highly valuable data sets or credentials of high-value individual.

Their earnings reflect the premium value which cybercriminals are willing to pay to purchase stolen data. The margin of error highlights the uncertainty in self-reported data from the cybercriminals. Their earnings can fluctuate based on factors such as market state, data quality and the age of the data sets [17].

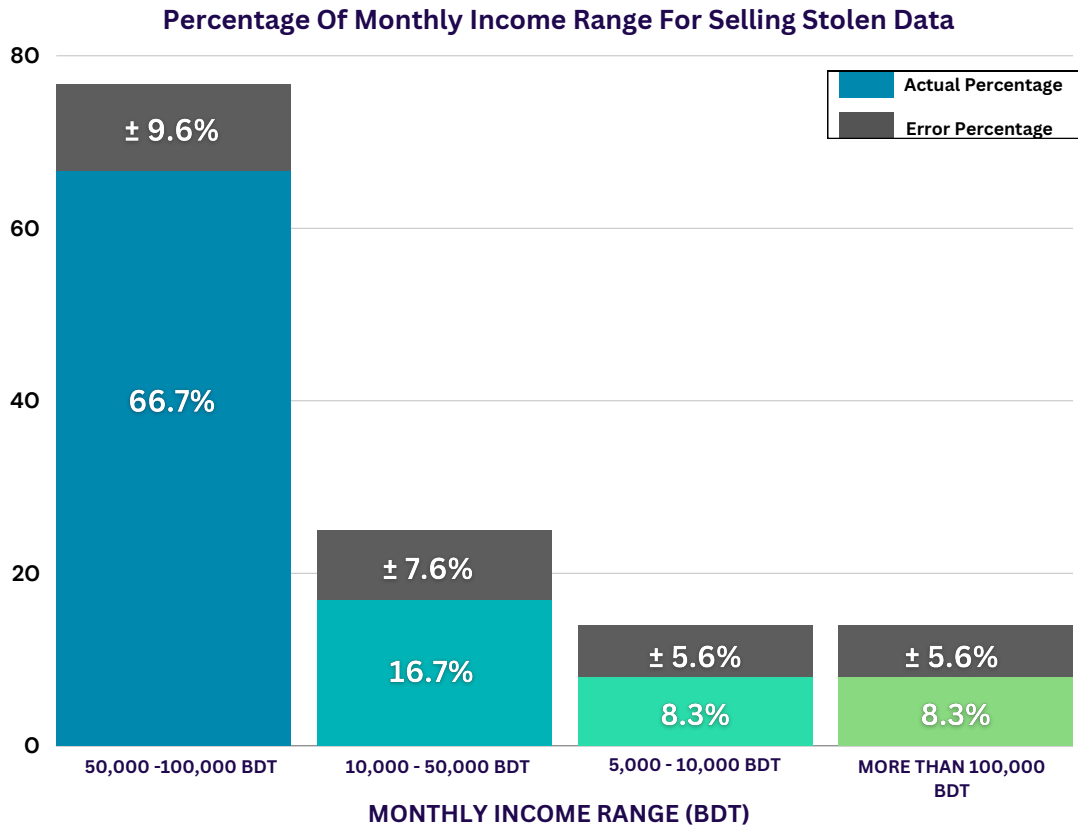


Figure 6.8: Monthly Income Range From Selling Stolen Data

Overall, the economic impact of botnets in Bangladesh is closely linked to unregulated digital transactions and a growing underground market. This is becoming an increasing threat to both the financial system and cybersecurity.

#### 6.1.4 Operational Techniques and Adaptability

The survey explores attackers adapting to use polymorphic/metamorphic malware to counter security measures. Figure 6.9 illustrates the propagation distribution for Drive-by-Downloads. Research has shown that phishing attacks, which involve tricking individuals into exposing sensitive information without knowing the risks of it. This is one of the most common successful methods used by cybercriminals as they gain leverage through psychological manipulation [18]. This form of attack is highly effective due to their exploitation of human vulnerabilities rather than focusing on the technical weaknesses in servers or devices [19].

From the pie chart 6.9, it has been revealed that approximately 70.5% of attackers opted for phishing and social engineering tactic due to its significant effectiveness in exploiting human vulnerabilities. The error of 11.1% indicates margin of error due to variable factors. While 11.8% attackers chose exploiting unpatched software as a method for propagation of malicious links. Attackers exploit vulnerabilities in software that has not been updated or patched, with a error margin of 7.8%. Using compromised devices to distribute malware payloads was cited by 5.9% of attackers. This sort of tactic typically involves leveraging hijacked devices to spread malware

without the users notice. While its slightly lower percentage compared to other tactics, exploiting network vulnerabilities was reported by 11.8% of attackers. This method involves taking advantage of flaws or loopholes in network configurations to hijack and spread malicious content.

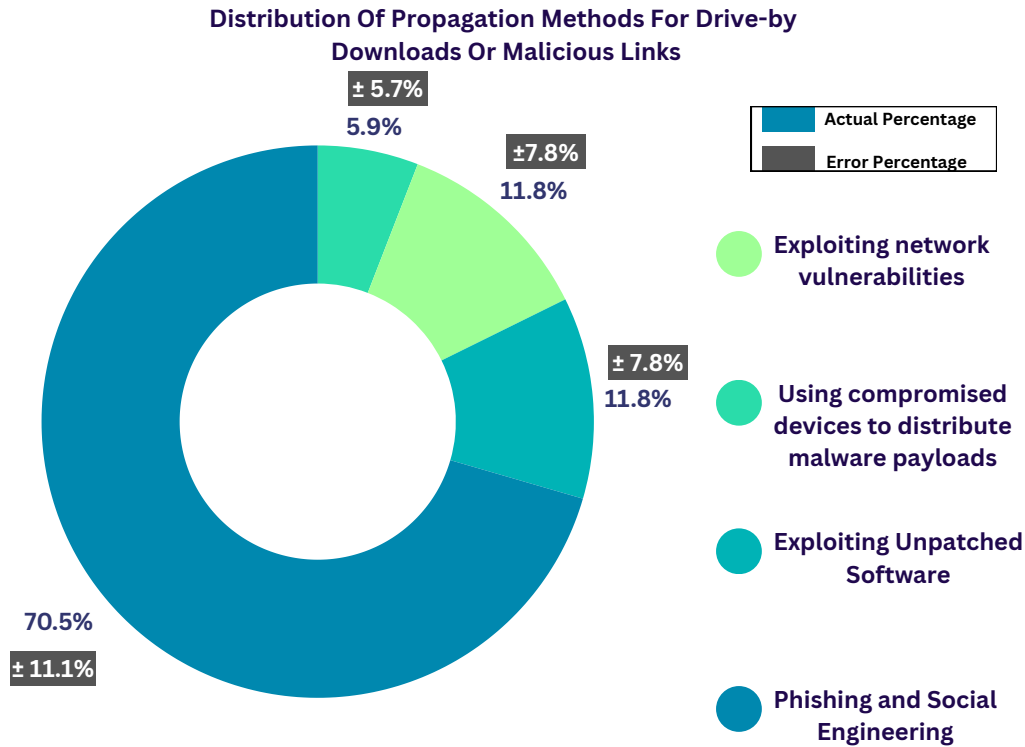


Figure 6.9: Propagation Distribution for Drive-by-Downloads

Tactics used by attackers with regard to security measures have been discussed. Figure 6.10 depicts the distribution of tactics used by attackers to adjust to security measures for polymorphic/metamorphic malware users.

35.7% attackers opted for Investing in Research and Development, indicating that they take a proactive approach to stay ahead of the security updates with a margin of error of  $\pm 12.8\%$ . Attackers invest in R&D to create polymorphic/metamorphic malware which changes its code dynamically, making it more difficult for the traditional security measures to detect and act upon [23]. 21.4% of attackers engage in continuous monitoring and analysis of security trends to stay ahead of defense mechanisms and adapt new tactics accordingly.

Moreover, by staying ahead they can find out the flaws in their malware and take counter steps against security updates [24]. 7.1% attackers indicated utilizing social engineering techniques to bypass human-based security controls, cybercriminals target exploitation of human vulnerabilities, with an error margin of  $\pm 6.9\%$ . Social engineering heavily relies on human error and might not always give consistent results [25]. Hence its the least chosen answer among attackers. These findings shed light on the adaptive strategies attackers take which can range from research and

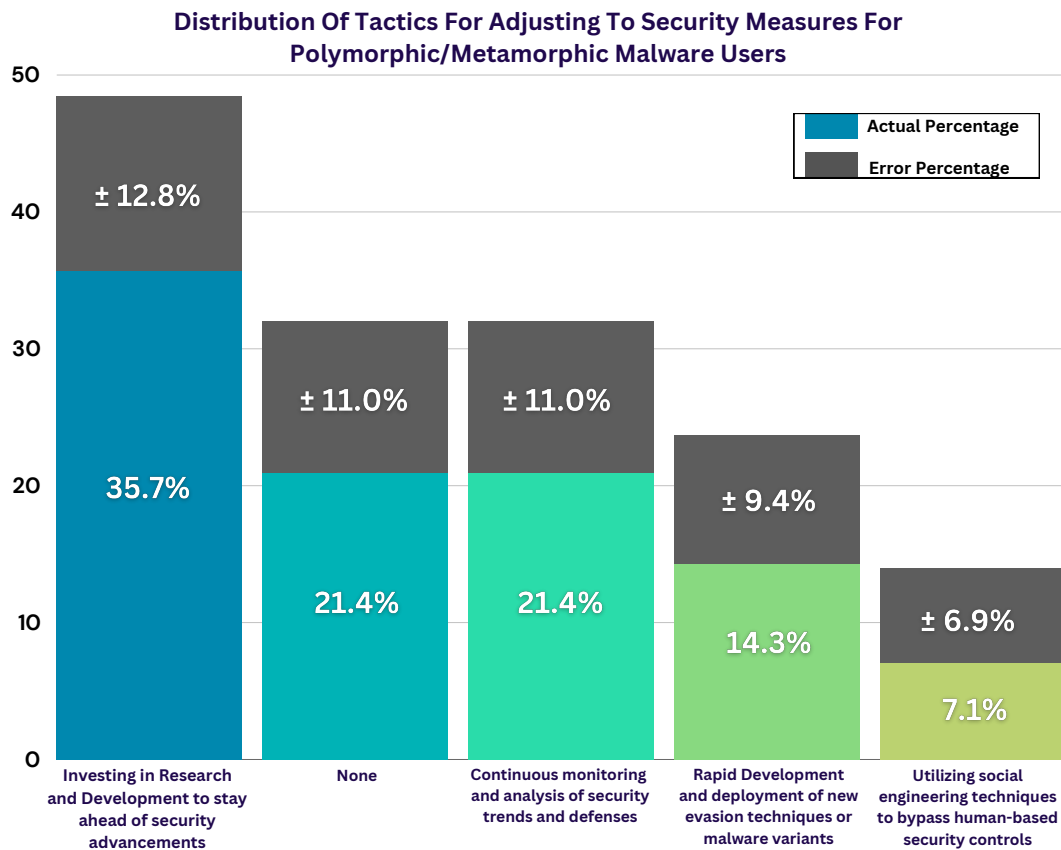


Figure 6.10: Tactics for Adjusting to Security Measures

development to exploiting social engineering tactics to adjust for evolving security measures. The margins of error indicate about the reliability of the survey results.

## 6.2 Hypothesis Testing for Attacker's Perspective

In this section, the study will delve into applying the chi-square test of independence to determine any associations between key variables and to test the hypotheses formulated beforehand. Details about the chi-square test of independence can be found in Chapter 3 of the Methodology of this report. The following sections will dive into details about the experimental design, study objectives, hypotheses, and lastly analysis and results.

### 6.2.1 Experimental Design

To get a detailed view of the attacker's perspective, data was gathered with specific emphasis on the role of botnet attacks carried out by cybercriminals and other various factors. The survey was meticulously designed to gather information by indirectly engaging with cybercriminals, ensuring that the questions addressed their real-world experiences and the challenges they face when managing botnets. The survey was distributed by reaching out to group admins in several hacking forums and online communities, resulting in 46 responses. This approach provided a comprehensive view of the hacker community's operation in Bangladesh. The confidentiality of the respondents was ensured to encourage honest and detailed answers,



thereby enhancing the integrity of the data collected. A detailed description of the survey design, participant selection, and statistical methods can be found in the Methodology Chapter of this paper.

### 6.2.2 Study Objectives

The primary reason for carrying out this study is to track down the impacts on the economy due to these malicious botnet attacks, which are specific to the Bangladeshi digital landscape. Consequently, insights into the operational challenges of managing botnets, the evolving tactics employed by cybersecurity breachers, their impact on cybersecurity, and consequently the stability of the economy were inspected. Therefore, the dataset collected is essentially a tool that can be used to design and develop certain schemes to significantly lessen the chaos of botnet attacks, as well as fortify precautionary measures in the field of cybersecurity, locally and globally.

### 6.2.3 Hypotheses

In understanding the attacker’s perspective, two central hypotheses were formulated to explore the factors that influence the behavior and strategies of botmasters:

- **Hypothesis 1:** Botmasters who target Bangladesh are more likely to spend more on infrastructure costs and employ a variety of evasion techniques compared to those who target other South Asian countries.
- **Hypothesis 2:** The monthly earnings of botmasters depend significantly on the method used to monetize botnet activities.

### 6.2.4 Results and Analysis

As mentioned in Chapter 3 of Methodology, the chi-square test of independence was applied to test the hypotheses in Section 5.2.3 as it allows to statistically assess whether the observed relations between variables are significant or not. The following sections of this Chapter will present the results of this experiment and their implications for the cybersecurity landscape in Bangladesh from the attacker’s point of view.

#### **Study 1: Target Selection, Primary Investment, and Evasion Techniques**

This study will examine the relationship between three critical variables that influence an attacker’s decisions. These variables are target selection, resource investment, and the use of evasion techniques. The study intends to determine whether there exists a significant association between the country being targeted, the area of investment, and the use of evasion tactics.

The study aims to identify whether attackers targeting Bangladesh allocate more investment towards infrastructures and employ evasion techniques as opposed to those who target other South Asian countries. Table 6.2.1 presents a contingency table that shows the observed frequencies of countries targeted, investment areas, and the use of evasion techniques. This table allows for the study to conduct further

analysis using chi-square test of independence.

**Table 6.2.1: Contingency Table of ‘Target’, ‘Primary Investment’, and ‘Use of Evasion Tactics’**

Target	Primary Investment	Use of Evasion Tactics		Column Total
		Yes	No	
Bangladesh	Infrastructure	8	6	14
	Others	3	9	12
Other SAC	Infrastructure	6	6	12
	Others	7	1	8
Row Total		24	22	46

The null and alternate hypothesis for this study is to be formulated in order to determine if the variables are associated in the following manner:

**Null Hypothesis ( $H_0$ ):** Botmasters targeting Bangladesh do not spend more on infrastructure costs and do not employ a greater variety of evasion techniques compared to those targeting other South Asian countries.

**Alternate Hypothesis ( $H_A$ ):** Botmasters who target Bangladesh are more likely to spend more on infrastructure costs and employ a variety of evasion techniques compared to those who target other South Asian countries.

Following the same approach as mentioned in Chapter 4, in order to verify the null hypothesis, a significance level  $\alpha = 0.05$  will be considered. Keeping the third variable as a controlling factor, the contingency table will be taken into partial tables of two variables which helps in determining whether the relationship of the two variables is independent of the third controlling factor. If the relationship between the two variables remains consistent across different levels of the controlling factor then it can be concluded that the three-variables are independent of each other. Now, the study will explore the relationship between targets and primary investment while keeping use of evasion tactic as a constant factor. Table 6.2.2 shows the observed frequencies for attacker targets and primary investment behind a botnet.

**Table 6.2.2: Observed Frequencies for variables ‘Target’ and ‘Primary Investment’**

Target \ Primary Investment	Infrastructure	Others	Column Total
Bangladesh	14	12	26
Other SAC	12	8	20
Row Total	26	20	46

Using these observed frequencies, the expected frequencies were calculated. The expected frequencies are shown in Table 6.2.3 for the variables ‘Target’ and ‘Primary Investment’.

**Table 6.2.3: Expected Frequencies for variables ‘Target’ and ‘Primary Investment’**

Target \ Primary Investment	Infrastructure	Others
Bangladesh	14.69	11.304
Other SAC	11.304	8.69

The chi-square statistic is then calculated using the formula referenced in Chapter 3 of the Methodology:

$$\chi^2 = \sum \frac{(O - E)^2}{E}$$

$$= 0.1729$$

Chi-square value,  $\chi^2 = 0.1729$

With 1 degree of freedom, the p-value is calculated to be 0.6764, which is greater than the significance level of 0.05. Therefore, the study fails to reject the null hypothesis, indicating no significant association between target and primary investment.

Similarly, the study investigates the relationship between target and use of evasion techniques, while keeping primary investment as the controlling factor. Table 6.2.4 shows the observed frequencies for attacker targets and use of evasion techniques to avoid detection.

**Table 6.2.4: Observed Frequencies for variables ‘Target’ and ‘Use of Evasion Tactics’**

Target \ Use of Evasion Tactics	Yes	No	Column Total
Bangladesh	11	15	26
Other SAC	13	7	20
Row Total	24	22	46

Using these observed frequencies, the expected frequencies were calculated. The expected frequencies are shown in Table 6.2.5 for the variables ‘Target’ and ‘Use of Evasion Tactics’.

**Table 6.2.5: Expected Frequencies for variables ‘Target’ and ‘Use of Evasion Tactics’**

Target \ Use of Evasion Tactics	Yes	No
Bangladesh	13.565	12.434
Other SAC	10.434	9.565

Chi-square value,  $\chi^2 = 2.33345$

With 1 degree of freedom, the p-value is calculated to be 0.1266, which is greater than the significance level of 0.05. Therefore, the study fails to reject the null hypothesis, indicating there is no association between between attacker target selection

and use of evasion tactics to avoid detection.

Lastly, while keeping target constant, the study investigates the relationship between primary investment and use of evasion techniques. Table 6.2.6 shows the observed frequencies for attacker’s primary investment behind a botnet and use of evasion techniques.

**Table 6.2.6: Observed Frequencies for variables ‘Primary Investment’ and ‘Use of Evasion Tactics’**

Primary Investment \ Use of Evasion Tactics	Yes	No	Column Total
	Infrastructure	14	12
Others	10	10	20
Row Total	24	22	46

Using these observed frequencies, the expected frequencies were calculated. The expected frequencies are shown in Table 6.2.7 for the variables ‘Primary Investment’ and ‘Use of Evasion Tactics’.

**Table 6.2.7: Expected Frequencies for variables ‘Primary Investment’ and ‘Use of Evasion Tactics’**

Primary Investment \ Use of Evasion Tactics	Yes	No
	Infrastructure	13.565
Others	10.434	9.565

Chi-square value,  $\chi^2 = 0.067$

With 1 degree of freedom, the p-value is calculated to be 0.7957, which is greater than the significance level of 0.05. Therefore, the study fails to reject the null hypothesis, indicating there is no association between primary cost and and evasion tactics.

**Result:**

1. Target & Primary Cost: No association
2. Target & Evasion Tactics: No association
3. Primary Cost & Evasion Tactics: No association

**Discussion:**

Since, all three-variables do not share any association with each other, the study fails to reject the null hypothesis which indicates botmasters targeting Bangladesh do not spend more on infrastructure costs and do not employ a greater variety of evasion techniques compared to those targeting other South Asian countries.

According to [47], motivated attackers are present in all countries of the world as internet lets them affect any device from anywhere in the world. These attackers choose their targets based on the potential risks and benefits. Moreover, it is to note that Bangladesh has a weak cybersecurity firewall and it is relatively easy to break in [50]. Therefore, attackers do not invest in their botnet infrastructure or deploy sophisticated evasion tactics as it is not necessary to infiltrate in Bangladesh's cyber landscape.

Therefore, the study fails to reject the hypothesis which suggests that there is no statistical evidence to support the claim that botmasters targeting Bangladesh invest more in infrastructure and use evasion techniques compared to those targeting other South Asian countries. These findings indicate that attackers are unlikely to prioritize Bangladesh over other regional targets regarding strategic primary investment or use of evasion techniques.

## **Study 2: Monetization Methods and Botmasters' Earnings**

In this study, the relationship between the monetization methods employed by botmasters and their monthly earnings will be examined. Understanding how different monetization strategies influence the financial gains of botmasters is crucial to shedding light on the economic drivers behind botnet activities. Table 6.2.8 presents the contingency table of observed frequencies, categorizing botmasters based on the methods they use to monetize their botnet operations and their corresponding monthly earnings.

The null and alternate hypotheses for this study are as follows:

**Null Hypothesis ( $H_0$ ):** There is no association between the monetization method and the monthly earnings from botnet activities.

**Alternate Hypothesis ( $H_A$ ):** There is an association between the monetization method and the monthly earnings from botnet activities.

Using these observed frequencies, the expected frequencies were calculated. The expected frequencies are shown in Table 6.2.9. for the variables 'Monetization Methods' and 'Monthly Earnings (BDT)'

Chi-square value,  $\chi^2 = 29.6061$

With 18 degrees of freedom, the p-value is calculated to be 0.0414, which is smaller than the significance level of 0.05. Therefore, the study rejects the null hypothesis which indicates that there is an association between the monetization method and the monthly earnings from botnet activities.

### **Result:**

- Monetization methods & Monthly earnings: Association

**Discussion:** The findings of this study indicate that there is a statistically signif-

**Table 6.2.8: Contingency Table of ‘Monetization Methods’ and ‘Monthly Earnings in BDT’**

Monetization Methods	Monthly Earnings (BDT)	5k-10k	10k-50k	50k-100k	More than 100k	Column Total
	Ransomware	0	1	3	0	4
Selling access	0	2	0	0	2	
Renting DDoS	1	1	0	3	5	
Selling data	2	4	16	2	24	
Distributing spam/phishing	0	0	3	1	4	
Botnet as a service (BaaS)	0	0	3	0	3	
Click/ad fraud	1	2	1	0	4	
Row Total	4	10	26	6	46	

**Table 6.2.9: Expected frequencies for variables ‘Monetization Methods’ and ‘Monthly Earnings in BDT’**

Monetization Methods	Monthly Earnings (BDT)	5k-10k	10k-50k	50k-100k	More than 100k
	Ransomware	0.347	0.869	2.26	0.521
Selling access	0.173	0.434	1.1304	0.2608	
Renting DDoS	0.434	1.086	2.826	0.652	
Selling data	2.086	5.217	13.565	3.1304	
Distributing spam/phishing	0.3478	0.869	2.2608	0.521	
Botnet as a service (BaaS)	0.2608	0.6521	1.6956	0.391	
Click/ad fraud	0.347	0.869	2.2608	0.521	

icant association present between the monetization methods employed by the botmasters and their monthly earnings. According to [51], botnets are used to generate revenue through several methods. In 2012, Russian hackers rented their botnets for \$30 - \$70 per hour for DDoS attacks, the Grum botnet earned \$2.7 million from spam campaigns, and the botmasters of Rustock botnet earned \$1.9 million annually from stealing data [51]. But for local botmasters, selling stolen data is the most profitable.

The result from this analysis suggests that the earnings are closely tied to the specific activities their botnet is used for. Certain activities are more profitable than others. The findings from this study also helps explain the motivations behind such criminal behavior as the potential for substantial financial gain drives many of these

illegal operations.

Therefore, this section explored and analyzed the investment behaviors and operational strategies of botmasters targeting Bangladesh. The study's findings did not provide sufficient statistical evidence to reject the hypothesis that botmasters targeting Bangladesh invest more in infrastructure or employ advanced evasion techniques compared to those targeting other South Asian countries. This suggests that attackers are unlikely to treat Bangladesh as a higher-priority target in terms of strategic investments or specialized evasion methods. However, the study uncovered a statistically significant association between the monetization methods used by botmasters and their monthly earnings. The data indicate that botmasters' income is directly influenced by the specific activities they employ their botnets for, with some methods proving to be more lucrative than others. These insights shed light on the underlying motivations for engaging in cybercriminal behavior, as the prospect of substantial financial gain is a key driver for many of these illegal activities. Understanding these economic incentives is critical in devising countermeasures to deter future botnet operations.

In conclusion, this chapter unveiled the operational tactics used by the local botmasters, target selection, the financial aspects of botnet operations, their source of information. From the data collected from 46 local botmasters, the research uncovered valuable insights regarding the attacker's behavior and trends followed for their botnet operations. From the hypothesis testing, it is uncovered that the monthly income generated from the botnet operations are closely linked to the monetization methods they employ. Furthermore, it is discovered that the botmasters do not require to spend more on the infrastructure of their botnets and employ sophisticated evasion tactics when they target Bangladesh as opposed to the other South Asian countries. Moreover, from exploratory data analysis, it is observed that most botmasters prefer to target overpopulated countries like India, Pakistan, and Bangladesh, while leaving out less populated countries like Sri Lanka, Maldives, Afghanistan, Nepal, and Bhutan. It is also found that botmasters primarily target government institutions, highlighting the vulnerabilities in Bangladesh's cyber defense. The primary objective of launching botnet attacks for most botmasters is to commense Trojan attacks which they mostly propagate through social engineering tactics. It is also found that, most attackers do not gather information on cybersecurity trends which highlights that these attackers are not sophisticated, whereas the ones who gather information mostly depend on incident reports which aren't likely from Bangladesh. The primary source of monetization comes from selling stolen data and most attackers make about 50,000-100,000 BDT from it monthly. Therefore, these key findings underscore the urgent need for enhanced cybersecurity measures and greater awareness to combat the evolving threats posed by local botmasters in Bangladesh.

# Chapter 7

## Security Expert's Perspective

In an increasingly interconnected world, the threat of botnets and cyberattacks has escalated and has become a huge threat to a developing nation like Bangladesh. Bangladesh in recent times has been facing unique challenges in defending its digital infrastructures. Pipeline Inc., a leading cyber defense company is at the front line tackling these challenges. They focus on mitigating botnet activities, enhancing cybersecurity vulnerable sectors such as government, healthcare, and financial institutions, and raising awareness. This chapter delves into a detailed discussion from a meeting held between representatives of Pipeline Inc., exploring the different types of cyber attackers and finding out the motivations behind these attacks and the strategies they have adopted to safeguard cyberspace. With limited resources and a lack of comprehensive support from law enforcement in Bangladesh, the company provides critical insights into the importance of raising cyber hygiene, innovating defensive technologies, and bridging the gap between people, processes, and technology. This analysis offers an important strategy to make Bangladesh's cyberspace more resilient.

The interview was conducted in person with two representatives from Pipeline Inc. The participants were Md. Mazharul Islam, Marketing Manager, and A.S.M. Shamim Reza, Chief Technology Officer. The interviewees were arranged through mutual contacts and the whole interview lasted approximately two hours.

### 7.1 Overview of Botnet Detection and Defense

The interview covered botnet's life-cycle, detection process, emergency response, and mitigation processes. According to Pipeline Inc., the key indicators of botnet infection include:

- Unusual outbound traffic from compromised devices.
- Communication with suspicious IP addresses or known command-and-control (C&C) servers.
- Lack of cybersecurity hygiene and awareness leading to mass network infection and theft of sensitive data.



Pipeline Inc. employs a strategy of using Intrusion Detection Systems (IDS) like Snort and Intrusion Prevention Systems (IPS) like Suricata to provide reactive security. However, more proactive monitoring and threat-hunting tools were recommended for future defense strategies [37].

## 7.2 Challenges in Botnet Mitigation and Cybersecurity Preparedness

The interviewees highlighted the challenges encountered in defending against botnets and implementing security frameworks across diverse industries. Pipeline Inc. emphasized the importance of integrating *people*, *processes*, and *technology* to create a solid defense against cybersecurity threats [37]. The core challenges included:

- **People:** Lack of awareness among people and insufficient cybersecurity training, particularly in government sectors makes these entities highly vulnerable and defenseless against botnet attacks.
- **Processes:** Deficit in tools required to log threats and run forensic analysis alongside the lack of post-attack mitigation strategies causes industries significant harm. Organizations often lack proper asset both software and hardware wise complicating the deployment of effective security solutions [37].
- **Technology:** The interviewees stressed the shortcomings of current and mostly used tools which are purely reactive based. Real-time monitoring and threat intelligence integration or proactive methods were suggested to stay ahead of threats and to detect and mitigate them from the early stages [37].

## 7.3 Financial and Operational Impact of Botnet Attacks

The financial and operational impacts of botnet attacks were also discussed during the interview. For instance, one Bangladeshi organization lost millions of dollars due to the compromise of its digital system during a ransomware attack which resulted in a week-long downtime [37]. Interviewees strongly emphasized the growing insider threats and human errors as one of the leading factors behind initial botnet infection. Attacks are motivated by financial gain, espionage, or competitive advantage. In Bangladesh, the fintech industry and government sectors are the primary targets. Competitors might take down their competition using cyber attacks or even steal and sell the data of their competitors [37].

## 7.4 Key Components for a National Cybersecurity Framework

To develop a comprehensive national cybersecurity framework, the interviewees recommended focusing on the following foundational components:

- **DNS Filtering:** Using and fine tuning DNS filtering to block malicious traffic [37].
- **Technology:** Incorporate IDS/IPS systems and proactive threat-hunting tools. Both reactive and proactive combined to make a solid stand against cybersecurity threats technologies [37].
- **Collaboration and Training:** Encourage collaboration among private organizations and the government to host regular cybersecurity training programs and build awareness campaigns to enhance the country's cybersecurity capabilities [37].

## 7.5 Recommendations for Enhancing Cybersecurity in Bangladesh

The interviewees provided several recommendations to improve Bangladesh's cybersecurity landscape:

### 7.5.1 People and Technology Insights

One of the biggest challenges in Bangladesh is the lack of cyber hygiene. Many individuals, particularly the older generation are quite resistant to adopting new technologies and strategies. They are not aware of the adverse effect of cyber threats such as Botnet. Education or Training campaigns both within companies and publicly can help this change. Cyber defense companies should focus on training employees and instilling better strategies and practices. In addition, regular workshops and courses should be offered to combat the hacking mentality among youth. Emphasis must be created for the importance of cybersecurity over cyberoffense [37]. Human error is often the weakest link in cybersecurity. The insider threat is particularly difficult to detect but it can easily be mitigated by imposing strict security measures, continuous monitoring of security protocols, and through strong company policies. Furthermore the collaboration between people and technology must be enhanced as well. For example:

- **Training and Human Resources:** Upskilling employees in cybersecurity practices and showing them adverse effect of bad practices.
- **Technological Advancement:** Implementation of advanced threat-hunting techniques using AI and machine learning. And using that data to find out abnormal data usage patterns and cross-referencing with threat intelligence [37].

### 7.5.2 Technological Innovation and Automation:

Developing AI-driven and ML Based threat hunting system can enhance cybersecurity. Automated tools can help reduce human errors and minimize the need for manual intervention. This will also result in limited access over less secured parts of a system reducing the number of insider threats or human manipulations [37]

### **7.5.3 Improving Law Enforcement Collaboration:**

In Bangladesh, Law Enforcement is very poor and lack the necessary strategies to protect its cyberspace. The interviewees stated that government doesn't directly collaborate with any non-government cybersecurity agencies and only takes complaints from victim. As a result, a lot of valuable insights and help from non-government agencies to protect Bangladesh and its cyberspace is not being used [37]. Improved collaboration between cyber defense companies both governmental and non-governmental bodies is essential for better threat detection and mitigation strategies against cyber threats. [37].

## **7.6 Conclusion and Policy Implications**

The interviewees highlighted the unique challenges that Bangladesh faces in protecting its cyberspace and defending its digital infrastructure, especially financial organizations against botnet attacks. Poor cybersecurity practices, limited resources, lack of budget in cybersecurity aspects, and lack of collaboration with law enforcement agencies further worsen these vulnerabilities. To address these issues, Bangladesh must focus on developing a dynamic and adaptive cybersecurity framework. This chapter underscores the importance of people's awareness regarding digital threats alongside their harmful impacts. Moreover, proactive measures include the integration of reactive threat-hunting techniques to protect critical infrastructures. As cybersecurity threats continue to evolve at a rapid speed, a dynamic and adaptive approach is vital to safeguard Bangladesh's digital ecosystem.

# Chapter 8

## Analysis & Discussion

### 8.1 South Asia vs Bangladesh Comparison

As seen in Chapter 5, among the South Asian countries, Bangladesh is targeted 56.5% of the times by local attackers. Meanwhile, India is targeted 100% of the times and Pakistan with 39.1% of the times. Interestingly, countries such as Nepal, Bhutan, Maldives, Afghanistan and Sri-Lanka are never targeted by the botmasters for inclusion. Figure 8.1 illustrates the botnet attack distribution of Bangladesh with respect to its neighbouring South Asian countries. As mentioned in Chapter 5, this behavior shows preference towards highly populated countries as it guarantees a higher success rate of their attack.

**Percentage of Attackers Targeting Bangladesh vs Other Countries**

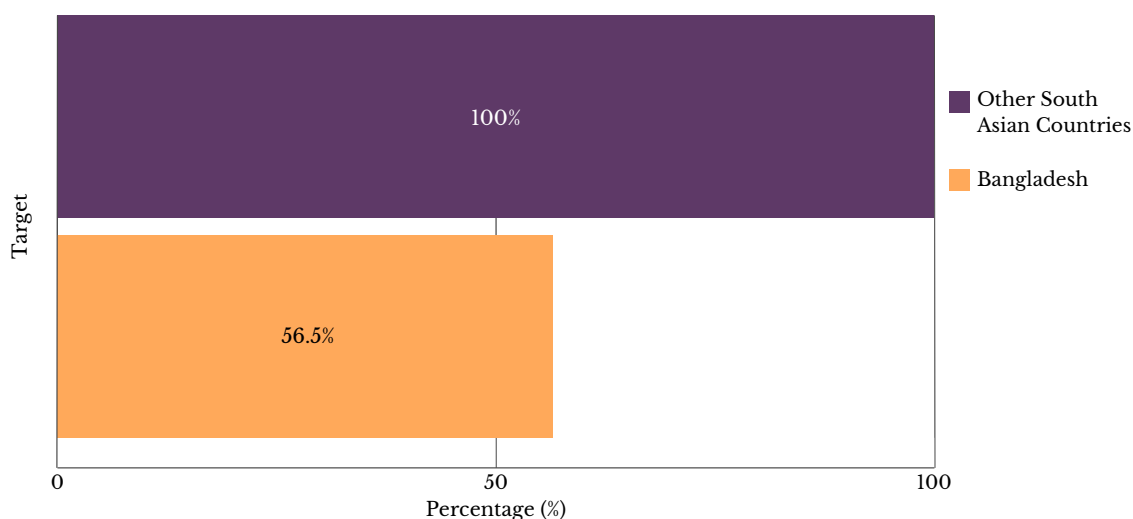


Figure 8.1: Botnet Attack Distribution Bangladesh Vs South Asian Countries

According to [6], since 2021 approximately 14,627 distinct IP addresses originating from Bangladesh have been identified as infected with malware, potentially indicating vulnerabilities that could be exploited as vectors for ransomware attacks. Bangladesh experiences an increase in cyber crimes from domestic and international

actors, with financial crimes like credit card fraud and digital money laundering on the rise. Over 63,000 cyber crime cases were reported in 2022, marking a 20% increase from 2021. Additionally, Bangladesh ranked as the 10th largest source of malware attacks and botnet operations globally, according to the Microsoft Security Intelligence Report of 2022 [63]. One such area that needs to be looked at is the nature of local cyber attackers' targets in Bangladesh. When analyzing the data gathered from the participants, a clear trend emerges: the attackers are highly inclined to target government institutions and other businesses, and only a small proportion of them prefers to target small businesses. Figure 8.2 presents distribution of targeted entities in Bangladesh with respect to other South Asian countries. The observed emphasis on governmental entities may give cause to concern over possible deficiencies in the nation's cybersecurity and its threats that extend to the delicate sphere of the governmental framework.

Furthermore, in 2019, three local private banks in Bangladesh fell victim to major cyber attacks [6]. Hackers managed to abscond up to USD 3 million from cash machines in Cyprus, Russia, and Ukraine by employing cloned credit cards. Besides, the BGD e-GOV CIRT also identified 3,639 bank cards from various banks that had been leaked Bangladesh banks are being targeted on cybercrime sites of the dark web. Furthermore, BGD e-GOV CIRT also revealed some notable weaknesses of the banking infrastructures which may be exploited by threat actors. These revelations agree with the conclusions as obtained from the collected data analysis.

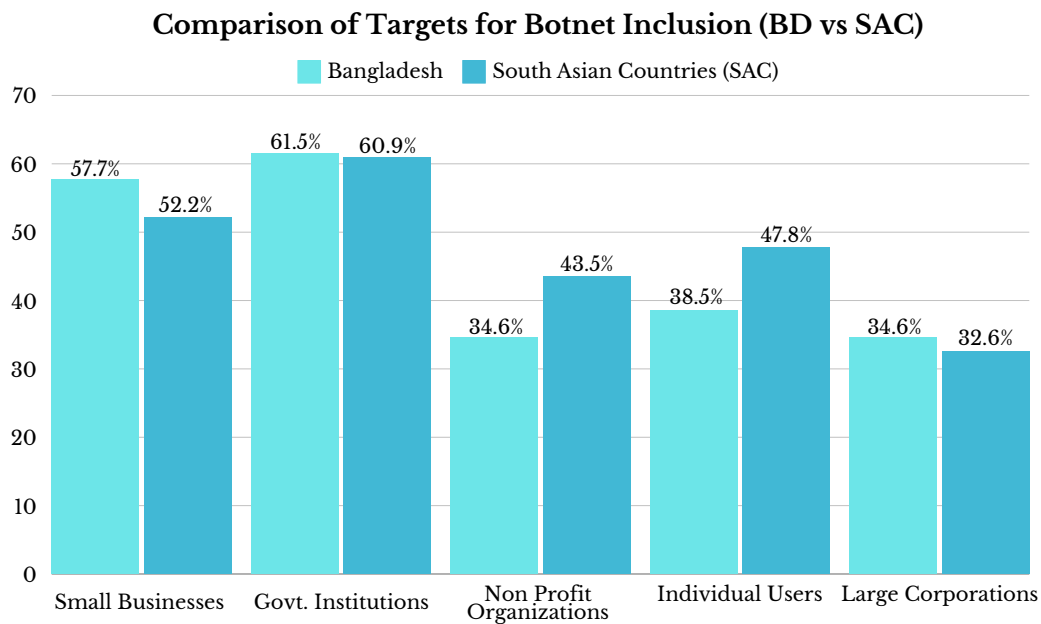


Figure 8.2: Targeted Entities Distribution Bangladesh Vs South Asian Countries

The percentage of government institutions, small businesses and large corporation being targeted remain slightly higher in Bangladesh than other South Asian countries combined. But in comparison, individual users and non-profit organizations remain less significantly lower targeted in Bangladesh than that of other South Asian countries. Figure 8.3 presents comparison chart of money generated by botnet attacks in Bangladesh with respect to other South Asian countries. Attackers

who target Bangladesh earn 50,000 - 100,000 BDT on average per month compared to attackers who target other South Asian countries earning on an average 10,000 - 50,000 BDT monthly. Besides that, the earning range for attackers targeting Bangladesh are drastically larger than attackers targeting other countries. Therefore, from this it is evident that local attackers leverage more money from targeting Bangladesh. Based on the gathered data and analysis, it is evident that

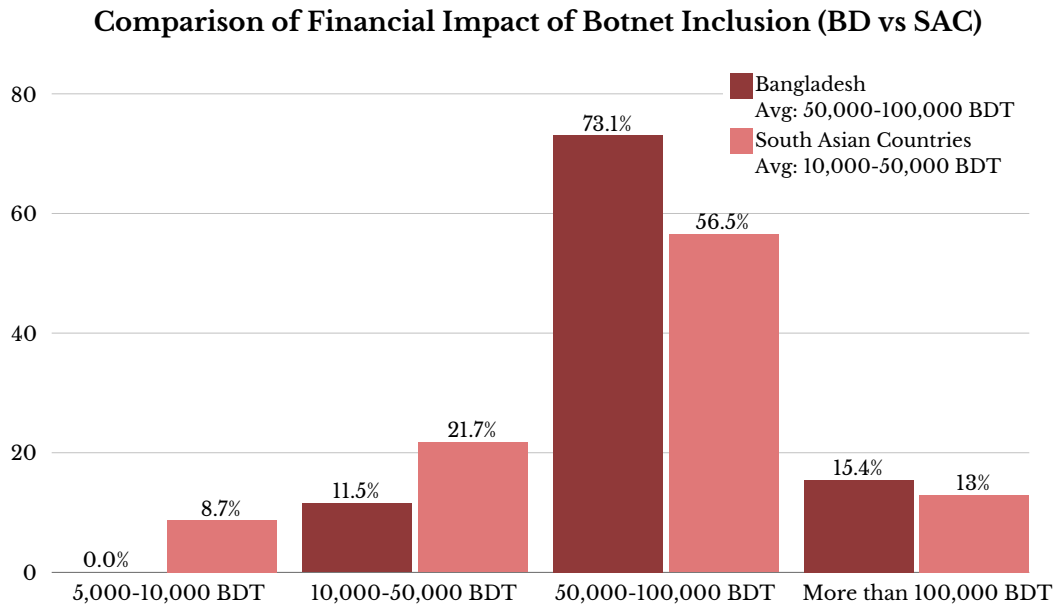


Figure 8.3: Comparison Chart of Money Generated By Botnet Attacks Bangladesh Vs South Asian Countries

Bangladesh faces a major cybersecurity threat against botnet attacks. Attackers leverage on selling stolen data from government institutions and small businesses. These attacks show vulnerabilities among the most pivotal entities in Bangladesh. Even though cryptocurrencies are illegal and thought to be banned, hackers opt for it to handle financial transactions in order to maintain anonymity. In conclusion, the findings highlight the weak cyber defence its been running on and emphasizes on the economic impact Bangladesh has been facing compared to other South Asian countries.

## 8.2 Global vs Bangladesh Comparison

This section presents the comparison between global findings and findings from this research on different aspects. The comparisons are done from the three perspectives of attackers, the general public and security experts. These insights will help highlight Bangladesh’s cybersecurity landscape in relation to the international context. It will also serve to validate the results of this study by highlighting both similarities and differences.

Table 8.2.1 summarizes the key differences and similarities between attacker perspectives in Bangladesh and global contexts. It highlights various aspects such as

monetization methods, targeted entities, income levels, and awareness of cybersecurity trends. This table provides insights into attackers' preference in targets, monthly revenue, primary goals, infrastructure costs, and security awareness in Bangladesh compared to worldwide patterns.

**Table 8.2.1: Comparison of Attacker Perspectives: Bangladesh vs Global**

Attribute \ Context	Bangladesh	Global
Monetization Methods	Most preferred monetization method is selling stolen data and financial information [Figure 6.7].	60% of the large scale DDoS attacks in 2024 are spread through botnets. Most botmasters monetize their operations through DDoS attacks globally [54].
Infrastructure Costs	Low spending on infrastructure [Chapter: 6.2.4].	Higher spending for stealth and evasion [51].
Target Preference	Focus on largely populated countries [Figure: 5.6].	Wealthy countries with large population guarantees higher success rates [47].
Primary Botnet Use	Trojan attack is the primary goal of local botmasters [Figure: 6.3].	Globally, botnets are primarily used for DDoS attacks [54].
Income Range	50,000-100,000 BDT/-month [Figure: 8.3].	Depending on the targeted countries and the operational methods, monthly income of botmasters vary globally. Although, it is significantly higher than the income of local botmasters [47].
Security Awareness	76.1% of the local attackers do not gather information on cybersecurity trends [Figure: 6.5].	Globally, attackers remain updated on trends and gather information on their targets [55].
Propagation Tactics	70.5% of the local attackers use phishing tactics [Figure: 6.9].	Globally, attackers rely heavily on social engineering tactics as 98% of the cyber crimes initiate through phishing [60].

Therefore, from the observed comparisons, it is evident that local and global botmasters both prefer to target countries with large populations. But most local attackers are outdated and do not gather cybersecurity information as opposed to most global attackers. Moreover, it is seen that the primary use of botnets for local attackers is to commence trojan attacks, whereas, for global attackers, their primary goal is to launch DDoS attacks. The global botmasters mostly monetize their botnets through DDoS attacks by offering them as a service, meanwhile the local botmasters monetize through selling stolen data. When it comes to infrastructure costs, the local attackers do not invest but the global attackers do. Although the average income of local botmasters are significant in the context of Bangladesh, in contrast, globally botmasters make more.

Table 8.2.2 outlines the major differences and similarities between the general public's perspective in Bangladesh and global contexts. The table explores multiple factors relating to the general public, including awareness and willingness to spend money, time spent online, device vulnerabilities, and education on cybersecurity. These comparisons shed light on the public's response to malware, trust in platforms, frequency of incidents, and behavior and attitudes toward cybersecurity, highlighting how they differ or align between local and global populations.

From the observed data, it is apparent that, from both the local and global public's perspective, there is a strong correlation between awareness of cybersecurity trends and willingness to spend money to stay protected. However, the gap between awareness and taking proactive measures, like regular updates, is still a challenge for Bangladesh. Interestingly, in comparison, the global average of time spent online by individuals is higher than that of Bangladeshi locals, who spend 4 - 8 hours per day online. Regarding device vulnerability, as the rise in smartphone penetration is constant for both populations, so is the surge in vulnerability. A concerning issue in Bangladesh is the lack of cybersecurity education, which mirrors the recent global trends. Despite this, in response to examining for malware, most locals run antivirus software while some ignore the potential threats, whereas, most global users are likely to follow the best practices. However, trust in online platforms diminishes for both local and worldwide populations after being compromised by cyberattacks or security breaches.

Table 8.2.3 shows the comparison between the perspective of the security experts in Bangladesh with global views. It focuses on key areas such as botnet threats, cybersecurity training, financial impact, and collaboration of government and private sectors. The table reveals the view of security experts on evolving botnet threats, their impact on the financial sector, and the necessary actions required to counter these threats in both local and global contexts.

As mentioned in the data table, local security experts report a surge in botnet threats, particularly targeting government and financial institutions. Botnet threats are also rising globally, especially affecting state-owned and financial organizations. Regarding cybersecurity training, the lack of sufficient training in Bangladesh is underscored, especially within government sectors. However, globally, there is a widespread gap in cybersecurity education. The financial impact of cyberattacks,



**Table 8.2.2: Comparison of Public Perspectives: Local vs Global**

Attribute \ Context	Bangladesh	Global
Awareness and Spending	Strong correlation present [Chapter: 5.2.4]	Willingness to spend money to stay protected is linked to awareness globally [47].
Updates and Awareness	No correlation with proactive updates [Chapter: 5.2.4]	Globally, awareness leads to safer practices [47].
Cybersecurity Incidents	36.03% of the respondents faced cyber incidents [Figure: 5.1]	Global rates vary but it is estimated to be very high since botnet attacks increased by 23% from the third quarter to the fourth quarter of 2021 [58].
Time Spent Online	About 50% of the respondents spend 4-8 hours/day [Figure: 5.3]	Globally, on average, individuals spends 6 hours and 31 minutes a day [59].
Device Vulnerability	46% use smartphones via Wi-Fi [Figure: 5.4]	About 96% of internet users globally use smartphones to browse the internet [59].
Cybersecurity Education	79% of the respondents are do not educate themselves on cybersecurity [Figure: 5.5]	Globally, lack of education remains a significant issue [47].
Response to Malware	Most run antivirus and some ignore threats [Figure: 5.7].	Individuals who faced cyber incidents in the past are more likely to follow best practices [47].
Trust in Platforms	75.6% fear botnets reduce trust [Figure: 5.8]	Globally, individuals have reported losing trust in online platforms that previously cyber incidents [61].

specifically ransomware, is another pressing issue. Significant losses were suffered due to ransomware in Bangladesh, but globally the problem is even larger, which resulted in the closure of small businesses. This comparison outlines that though Bangladesh faces significant financial losses, the global scope of ransomware attacks is causing even more widespread economic disruption. Finally, for collaboration, security experts in Bangladesh stress the urgent need for partnerships between government and private sectors to improve cybersecurity efforts and mitigate risks, which is a practice already in place globally. In conclusion, attackers in both local

**Table 8.2.3: Comparison of Security Expert Perspectives: Local vs Global**

Attribute \ Context	Bangladesh	Global
Botnet Threats	Threats are increasing and affecting government and financial institutions [37].	Globally, botnet threats are rising, targeting state owned and financial institutions [58].
Cybersecurity Training	Insufficient training, especially in govt sectors [37].	Global gap in cybersecurity education [47].
Financial Impact	Significant losses due to ransomware attacks [37].	In the first half of 2022, 236.1 million ransomware attacks were spread globally, even shutting down small businesses [62].
Collaboration	Need for govt-private partnerships [37].	Globally, private and government sectors work together to mitigate risks [47].

and global contexts prefer to target countries with larger populations, with global attackers generally using expensive infrastructures. The general public in both contexts shows a rising awareness of cyber threats but there still is a gap in proactive measures like cyber education and cyber hygiene. Finally, as security professionals recommended the need for improved training programs, enhanced collaboration, and stronger defenses against cyberattacks like ransomware are the key concerns both locally and globally. By addressing these challenges, a more resilient cybersecurity landscape could be built for safeguarding against cyber threats and future risks.

### 8.3 Key Findings and Discussion

From the analysis and hypothesis testing done so far, it is evident that the alarming rise in botnet-related cyber threats illustrates a troubling connection between the activities of the attackers, the vulnerabilities of the general public, and the insights of security experts. It is discovered that the local botmasters are driven by profit which is why they target government institutions due to their relatively weaker defenses as opposed to large corporations. This strategy reflects a calculated choice as they will be able to exploit the sensitive data within these sectors. Their operations yield significant income which averages from 50,000 BDT to 100,000 BDT per month which highlights the lucrative aspect of launching these botnet attacks. Moreover, the attackers' preference for social engineering tactics which exploits human vulnerabilities aligns with the findings from the general public's analysis highlighting a lack of awareness and education about cybersecurity.

The people who often remain unaware of the risks associated with their online behavior inadvertently contribute to the attackers' success. Even though a fraction

of the respondents acknowledges the threats of botnets, they still partake in risky online practices, such as downloading cracked software and neglecting to update their systems. This disconnection between awareness and action is directly helping the botmasters to intrude in their systems. The findings indicate that 36.03% of the respondents have experienced cybersecurity incidents which underscores the urgent need for increased public education on safer online practices and awareness on cyber attacks.

Moreover, from the interview with the security experts, it is revealed that the very system that's designed to protect these vulnerable government institutions and financial sectors, are insufficient. According to experts' opinion, there is a significant gap in cybersecurity training within government sectors which further escalates the issue. They highlight the critical need for proactive measures such as the integration of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). The lack of real-time monitoring and threat intelligence would be crucial for safeguarding these vulnerable and most targeted sectors.

Furthermore, it is notable that 76.1% of the attackers do not stay updated on cybersecurity trends, suggesting that they are mostly relying on outdated tactics. These outdated techniques only thrive in an environment of ignorance and complacency among the victims or the public. This dynamic creates a fertile ground for exploitation as attackers face little to no resistance from a public that has not received adequate cybersecurity education.

In conclusion, Bangladesh has rapidly adopted digital services across all sectors at an extraordinary pace. Few nations globally have experienced such swift digital integration among their population. However, with rapid transformation often comes increased vulnerability [39]. Addressing this vulnerability through well-crafted policies is generally seen as a long-term solution. Therefore, it is evident that the integration of people, process, and technology is essential to fortify the defenses against botnet attacks. Security experts advocate for an approach that includes public education campaigns, enhanced training for organizations, and the adoption of robust technologies for threat detection. Drawing insights from successful frameworks such as those in Singapore could be taken into consideration while crafting a framework model for Bangladesh. This strategy will not only address the immediate threats posed by the attackers but also empower victims with the knowledge and tools necessary to protect themselves. This ultimately creates a more resistant cybersecurity posture for the nation.

# Chapter 9

## Technical Evaluation

As botnet attacks continue to rise globally, Bangladesh is not also immune to its adverse impact. To safeguard the cyber space of Bangladesh and its cyber infrastructures, implementing a robust detection and mitigation framework is very crucial. This chapter delves into an integrated framework aimed at enhancing the detection and mitigation of botnet threats in Bangladesh. This framework mainly leverages based on existing Intrusion Detection Systems (IDS) and Host-based Intrusion Detection Systems (HIDS). A critical evaluation of tools like Snort, Suricata, and OSSEC highlights key challenges, while an integrated solution to improve detection accuracy and system performance is proposed. By deploying these tools in a controlled environment, this research aims to highlight the strengths and weaknesses of the tools which contributes to valuable data for Bangladesh's cybersecurity framework. The results obtained from this evaluation directly support the proposed framework for enhancing defense against botnet threats.

### 9.1 Technical Evaluation of Existing IDS/HIDS Tools

To effectively find a solution that will help automatically detect and mitigate against botnet attacks, we evaluated three prominent IDS/HIDS solutions. They are Snort, Suricata, and OSSEC. Each tool was tested in terms of its detection capabilities, ease of deployment, scalability, and resource efficiency. The following subsections describe the software's shortcomings and areas of improvement. The system on which the experiment was conducted had been configured with a 4 core Ryzen 5 5600X CPU and 8 GB of DDR4 memory to evaluate the performance of the tools.

### 9.2 Snort

#### **Disadvantage 1: High False Positive Rate**

Snort, a widely used IDS, operates using signature-based detection method. This method can cover a huge range of known threats and successfully mitigate them. But when a sheer volume of data is presented to it, its efficiency falters and as a result distinguishing between legitimate and botnet traffic becomes difficult. Hence, false positives are often generated due to large data volume [38]. WEB-IIS view

source via translate header is often detected as potential threat in snort. As a result, the false positive percentage of snort in this aspect is quite high. Fine tuning is required against all kinds of threats to increase accuracy of snort but it still is an issue as it can reduce the false alarm rate but it can also bring the risk of missing real attacks [38]. This is critical in real-time environments where false positives can result in overwhelming alert volumes and delayed responses to actual threats.

**Disadvantage 2: Performance Overhead** Performance degradation under heavy traffic load or huge volume of traffic for example in case of DDOS attack is another drawback observed in Snort. During a DDOS experiment Snort struggled to handle the high-throughput environment which resulted in delayed detection result and sometimes missed a lot of actual threats. In Bangladesh, where large-scale attacks may target critical infrastructure, this performance degradation presents a significant challenge.

The test was conducted with and without snort running. The test was performed on the system without snort running and attacked with ICMP flood a form of DDOS attack on the test machine. System performance and usage of the test machine were recorded while the DDOS attack was in progress. Again the test was conducted with snort enabled and added custom rules to snort to make it detect the DDOS attack and mitigate it. The result was recorded and compared with the data before snort was enabled.

1. Snort was initiated using the command:

Snort Command

```
sudo snort -A console -c /etc/snort/snort.conf -i enp0s3 -l /var/log/snort
```

2. System performance metrics, including CPU and memory usage, were monitored using the 'dstat' tool with the following command:

dstat Command

```
dstat --cpu --mem --top-cpu --top-mem
```

3. The ICMP flood attack was generated using the 'hping3' tool to simulate heavy traffic on the network interface. The attack was initiated with the command:

hping3 Command

```
sudo hping3 -c 100000 -d 120 -S -w 64 -p 80 -flood -rand-source 192.168.0.10
```

The table 9.2.1 depicts the resource usage of a system during an ICMP flood attack, before and after enabling Snort. And the figure 9.1 shows the system performance graph during a certain period of time (1-3)points.

**Table 9.2.1: System Performance Before and After Enabling Snort during ICMP flood attack**

Metrics	Before Snort	After Snort
User CPU (%)	9-10%	17-40%
System CPU (%)	19-22%	18-29%
Idle CPU (%)	65-70%	22-57%
Wait CPU (%)	0%	0-1%
Memory Used (MB)	999-1007MB	1932M-1943MB
Memory Free (MB)	5141-5149MB	4998M-5005MB
Buffered Memory (MB)	33MB	32MB
Cached Memory (MB)	1546-1549MB	776M-781M
Top CPU Process	hping3 (25%)	hping3 (24-25%)
Top Memory Process	gnome-shell (430MB)	snort (478MB)

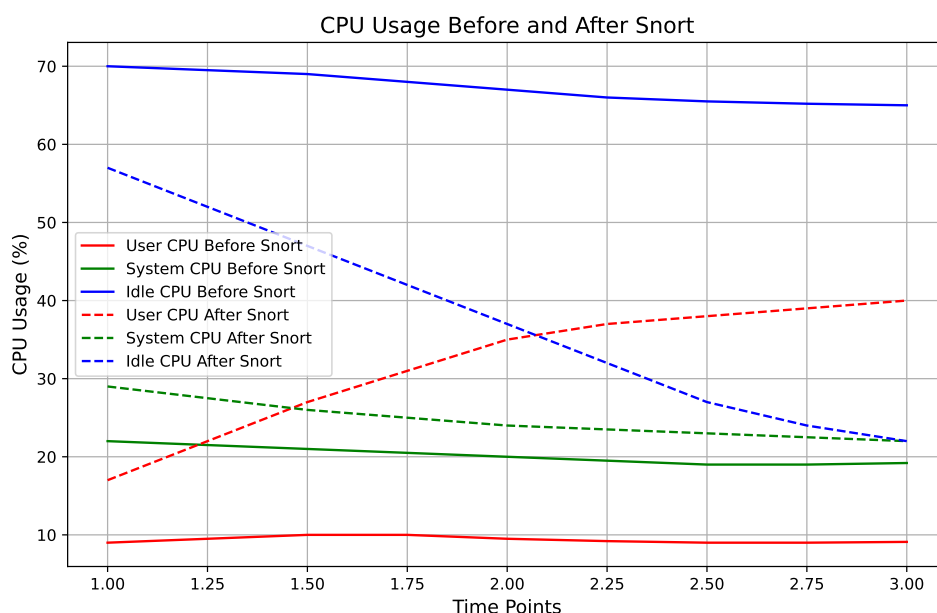


Figure 9.1: Server Performance During ICMP flood. Before vs After Snort

**Disadvantage 3: Signature Maintenance** Snort heavily relies on updates and maintenance to keep it operational. And maintaining an up-to-date and comprehensive signature set is a resource-intensive task. With botnets evolving every minute, it becomes hard to keep the tool up-to-date. Hence manual signature update can turn into an operational burden. New variants of botnets can remain undetected until their signatures are updated, leaving systems vulnerable during this gap.

Automating the signature update process can mitigate these challenges. The following pseudo code outlines a basic framework for automation:

### Pseudo Code: Automating Signature Updates

```
function updateSignatures():
    while true:
        if newSignaturesAvailable():
            downloadAndDeploySignatures()
        wait(X) ## wait for a defined period
```

To automate the update process Crontab can be used to check for signature updates after a certain time everyday.

#### 1. Open the Crontab Editor:

##### Crontab Command

```
crontab -e
```

#### 2. Add a Cron Job: To schedule a script that runs the ‘updateSignatures’ function every day at 3 AM.

##### Cron Job Command

```
0 3 * * * /etc/snort/update_signatures.sh
```

#### 3. Save and Exit: Save the changes and exit the editor. The cron job will run the script every day at 3 AM.

By implementing such automation, organizations can enhance their detection capabilities and reduce the risks associated with outdated signatures. It still leaves some room for flaws as the function has to wait a certain interval for example a day, so the time gap between a day to day is still a lot and the server could get affected by a threat that has been patched but the system doesn’t have it yet. Again reducing the time interval between updates can hamper productivity and if its too frequent, lots of computational resources will be wasted by Snort.

## 9.3 Suricata

### Disadvantage 1: Complex Configuration

Suricata offers advanced capabilities such as multi-threading, but this feature comes with a cost of complexity. The configuration process is not user-friendly and because of this mis-configuration or leaving loopholes behind while setting up is very likely to occur if not done properly. Suricata's configuration, particularly with tuning options like the `suricata.yaml` file can be a bit complex and not user friendly. Advanced settings such as adjusting packet processing modes or even optimizing configurations for specific multi-threading scenarios will certainly require in-depth knowledge of the system architecture [40].

### Disadvantage 2: Resource Intensive

Multi-threading mechanism is a resource intensive task utilizing all the threads or core of the processor. As a result it gets harder to handle large volume of traffic more efficiently than Snort. As it takes up more CPU and memory resources, it becomes difficult to implement in low-end systems or resource-constrained environments. For a developing nation like Bangladesh, reserving budget to purchase high end devices that can handle multi-threading tasks might be a far fetched idea which could limit its wide adoption. The experiment was conducted to observe the impact of Suricata on the resources of a system during an ICMP flood attack using `hping3`. The CPU and memory usage with and without Suricata was monitored.

1. Suricata was initiated using the command:

```
Suricata Command
```

```
sudo suricata -c /etc/suricata/suricata.yaml -i enp0s3
```

2. System performance metrics, including CPU and memory usage, were monitored using the `dstat` tool with the following command:

```
dstat Command
```

```
dstat --cpu --mem --top-cpu --top-mem
```

3. The ICMP flood attack was generated using the `hping3` tool to simulate heavy traffic on the network interface. The attack was initiated with the command:

```
hping3 Command
```

```
sudo hping3 -c 100000 -d 120 -S -w 64 -p 80 -flood -rand-source  
192.168.0.10
```

The table 9.3.2 depicts the resource usage of a system during an ICMP flood attack, before and after enabling Suricata. And the figure 9.2 shows the system performance graph during a certain period of time (1-3)points.



**Table 9.3.2: System Performance Before and After Enabling Suricata during ICMP flood attack**

Metrics	Before Suricata	After Suricata
User CPU (%)	9-10%	12-31%
System CPU (%)	19-22%	21-29%
Idle CPU (%)	65-70%	25-56%
Wait CPU (%)	0%	0-19%
Memory Used (MB)	999-1007MB	1190-1255MB
Memory Free (MB)	5141-5149MB	5093-5730MB
Buffered Memory (MB)	33MB	31MB
Cached Memory (MB)	1546-1549MB	795-1355MB
Top CPU Process	hping3 (25%)	Suricata-Mai (25%-41%)
Top Memory Process	gnome-shell (430MB)	gnome-shell (405MB)

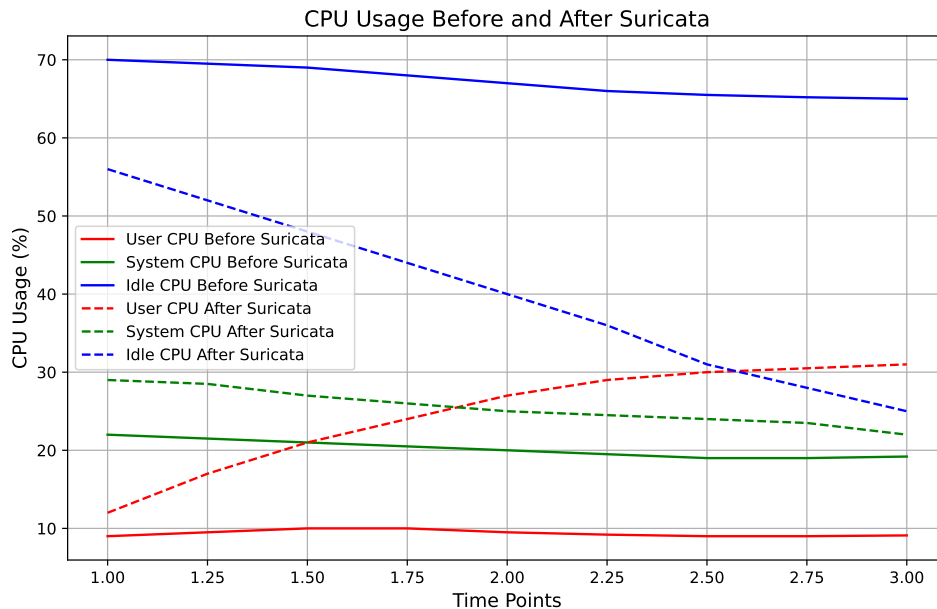


Figure 9.2: Server Performance During ICMP flood. Before vs After Suricata

### Disadvantage 3: False Positives and Tuning

Unlike Snort, Suricata does not use signature based detection. As a result sometimes it misses potential harmful traffic if not properly tuned. Regular updates to detection rules and parameters are required to minimize these kind of flaws. The time and expertise needed to continuously adjust these configurations can be a barrier to effective deployment. Suricata may generate a significant number of false positives if not tuned correctly which can overwhelm the system administrator. This requires constant monitoring and rule optimizations to reduce the percentage of false alarm rate [40]. For high-traffic environments lot of fine tuning is required to reduce false positive and correctly detect malicious traffic.

## 9.4 OSSEC

### **Disadvantage 1: Limited Network Detection**

OSSEC a host-based IDS (HIDS), focuses mainly on log monitoring and file integrity but it lacks the network traffic analysis which is vital in order to detect botnet activities in real-time. As botnets often rely on communication through network protocols, OSSEC alone is not sufficient to detect and mitigate the threat of botnets. OSSEC does not have the capability to monitor network traffic eventually making it ineffective against network-based threats like botnets [52].

### **Disadvantage 2: False positive**

In large-scale deployments OSSEC can struggle with scalability and produce false positives. With the increase in number of monitored hosts, managing and analyzing the data from multiple sources becomes very challenging. This is a critical limitation for environments with extensive IT infrastructures such as financial institutions or banking agencies. Events like a user repeatedly attempting to log in with an outdated email or password may trigger OSSEC to block that user's IP address. Even though no malicious intent is present such false positives can lead to service disruptions and require human intervention to re-establish normal operation [53].

### **Disadvantage 3: Performance Degradation**

One of the disadvantages of OSSEC lies with system performance. When real-time monitoring and analysis happen especially in complex environment and when dealing with large volume of malicious traffic, OSSEC can cause noticeable performance degradation. This usually happens due to the resource intensity of monitoring traffic, analyzing logs and generating alerts [56]. As a result end-user may experience slower system responsiveness in crucial moments.

## 9.5 Integrated Solution: Combining Snort and Suricata

To address the limitations observed in Snort and Suricata, we propose an integrated solution that leverages the strengths of both systems.

### **Advantage 1: Lower False Positive And Improved Detection Rate**

By combining Snort's broad signature-based detection with Suricata's advanced detection methods the false positive rates can be drastically reduced. Suricata's context-based and protocol-aware capabilities allow it to better distinguish between legitimate traffic and botnet activity. In this framework, Suricata would serve as the first layer of detection where Suricata would be working with a huge volume of data while Snort will be identifying known threats improving detection accuracy.

Snort and Suricata both have their strengths and weaknesses in detecting different types of attacks under stress. Suricata successfully identifies threats missed by Snort such as *ms01\_033\_idq* exploit due to Snort's nature of higher false negative

under stressed CPU state. While Snort excels at certain conditions where Suricata fails due to its higher resource demand [44]. Snort's lighter system load and its ability to handle single core environments makes it more efficient than Suricata but on the other hand Suricata's multi-threaded design allows it to perform significantly well in environments with multiple cores. This combined usage of both tools could help diminish each tool's individual weakness resulting in improved detection and reducing chance of false positives.

### **Advantage 2: Improved Performance Under Load:**

Suricata's multi-threading capabilities can help mitigate performance bottlenecks. By equally distributing the processing load across multiple threads or cores, it can handle high traffic volumes for example in case of DDOS attack. Snort, when deployed alongside Suricata, requires fewer resources as Suricata can absorb much of the heavy lifting in terms of high-traffic detection. The performance experiment with Suricata and snort and its process have been described.

1. Snort and Suricata were initiated using the following commands:

#### Suricata Command

```
sudo suricata -c /etc/suricata/suricata.yaml -i enp0s3
```

#### Snort Command

```
sudo snort -i enp0s3 -c /etc/snort/snort.conf
```

2. System performance metrics, including CPU and memory usage, were monitored using the `dstat` tool with the following command:

#### dstat Command

```
dstat --cpu --mem --top-cpu --top-mem
```

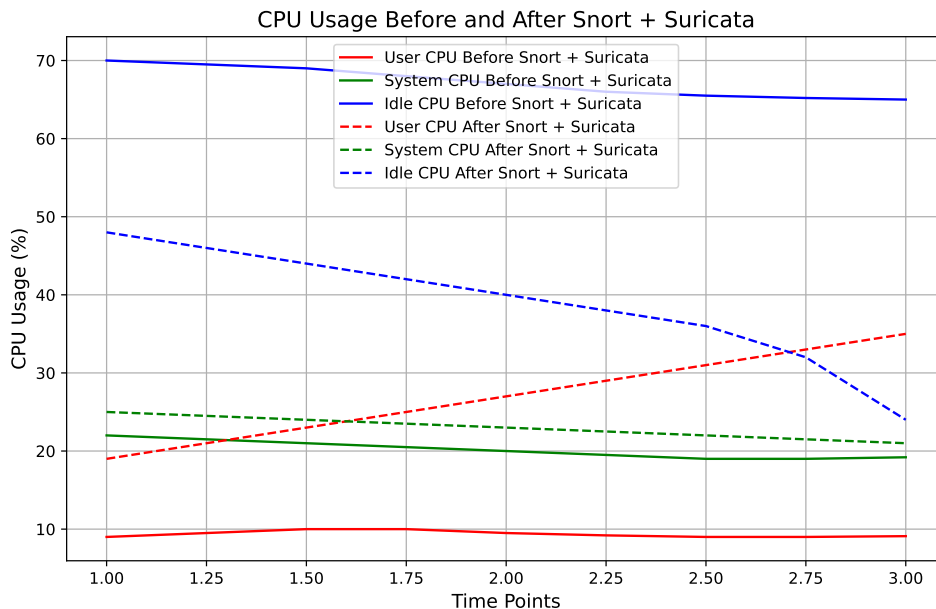
3. The ICMP flood attack was generated using the `hping3` tool to simulate heavy traffic on the network interface. The attack was initiated with the command:

#### hping3 Command

```
sudo hping3 -c 100000 -d 120 -S -w 64 -p 80 -flood -rand-source 192.168.0.10
```

Metrics	Before Snort/Suricata	After Snort + Suricata
User CPU (%)	9% - 10%	19% - 35%
System CPU (%)	19% - 22%	19% - 25%
Idle CPU (%)	65% - 70%	24% - 48%
Wait CPU (%)	0%	0% - 19%
Memory Used (MB)	999MB - 1007MB	2169M - 2213M
Memory Free (MB)	5141MB - 5149MB	4053M - 4378M
Buffered Memory (MB)	33MB	35M
Cached Memory (MB)	1546MB - 1549MB	1157M - 1429M
Top CPU Process	hpin3 (25%)	hping3 (25%)Suricata(26% - 37%)
Top Memory Process	gnome-shell (430MB)	snort (478M)

**Table 9.5.1: System performance comparison during a DDoS attack before and after running Snort and Suricata.**



**Figure 9.3: Server Performance During DDoS attack Before vs After Snort + Suricata**

The resource usage of the system is shown in Table 9.5.1. A comparison of performance metrics in Tables 9.2.1 and 9.3.2 highlights that even during high volume malicious traffic attacks, the system running both Snort and Suricata exhibits similar CPU and memory consumption compared to when each of the software is run independently.

Figure 9.3 illustrates the resource usage over the certain time interval (1-3) points. No abnormal spikes appeared during the whole process and the system remained stable throughout the attack period. These findings suggests that running Snort and Suricata concurrently is resource-efficient.

### Advantage 3: Signature and Rule Maintenance

Combining Snort-Suricata can benefit from shared features. Snort with its broad-based detection of known threats alongside Suricata's flexible rule sets can be more easily configured for defense against botnet attacks. This reduces the manual maintenance required to keep up with botnet evolution. Automation scripts can also be implemented to get regular updates without the need for too much human intervention.

#### Update Snort and Suricata Signatures Pseudocode

```
function updateSignatures():
    while true:
        if newSignaturesAvailable():
            downloadAndDeploySignatures()
            wait(X) # wait for a defined period
function downloadAndDeploySignatures():
    execute("wget -O /etc/snort/rules/snort.rules URL")
    execute("tar -xvzf /etc/snort/rules/snort.rules
-C /etc/snort/rules/")

    execute("wget -O /etc/suricata/rules/suricata.rules URL")
    execute("tar -xvzf /etc/suricata/rules/suricata.rules
-C /etc/suricata/rules/")

    print("Signatures updated successfully.")
```

Automating the process to check for update everyday at 3AM.

#### 1. Open the Crontab Editor:

##### Crontab Command

```
crontab -e
```

#### 2. Add a Cron Job: To schedule a script that runs the 'updateSignatures' function every day at 3 AM.

##### Cron Job Command

```
0 3 * * * /etc/snort/update_script.sh
0 3 * * * /etc/suricata/update_script.sh
```

#### 3. Save and Exit: Save the changes and exit the editor. The cron job will run the script every day at 3 AM.

Using both Snort and Suricata has its benefit as they both complement each other strengths and weaknesses. Improved performance under heavy traffic as found in [9.5.1](#) is crucial for live environments, especially in financial industries where downtime can cause significant damage to the economy. Moreover, enhanced detection accuracy helps end-users to experience an uninterrupted service. Suricata's advanced

protocols and anomaly detection enhance the precision of threat identification which complements Snort's signature-based approach leading to higher accuracy in detection. This also means if one system misses a threat, the other tool may successfully detect it increasing the overall robustness of the IDS setup. Furthermore, from figure 9.3 running both tools in parallel shows that system performance remains stable throughout heavy load attacks and can also provide an opportunity for load balancing where network traffic can be split between snort and Suricata, improving system performance and reducing latency.

In conclusion, this chapter highlights the effectiveness and limitations of existing intrusion detection systems such as Snort, Suricata and OSSEC in defending against botnet threats. By analyzing the key performance metrics and vulnerabilities, a combined solution using Snort and Suricata has been proposed. However, the operational challenges particularly the complexity of configuration and the need for higher specifications hardware due to their nature of being resource intensive depicts the need for further refinement. This evaluation sets the baseline for developing a more robust and scalable cybersecurity framework that can detect and mitigate botnet threats in Bangladesh's digital landscape.

# Chapter 10

## Proposed Framework for Bangladesh

This chapter covers details on criticisms of the current cybersecurity framework of Bangladesh, security experts' recommendations, strengths of Singapore's cybersecurity framework, and lastly, the proposed framework for Bangladesh to protect against botnet attacks. The framework will be incorporated by assessing the gaps in the current framework and focusing on the local security experts' opinions. Moreover, it will take inspiration from Singapore's cybersecurity framework as it has been consistently ranked among the top for cybersecurity preparedness. Further details can be found in the following sections of this chapter.

### 10.1 Existing Cybersecurity Framework of Bangladesh and its Gaps

Bangladesh has a sizable population of over 160 million people, with internet users numbering around 100 million as of 2021. The government has prioritized digitization across sectors like finance, commerce, education, and public services through initiatives like Digital Bangladesh [63]. As internet penetration grew in Bangladesh, cyber security threats evolved from simple website defacements by amateur hackers to conducting financial crimes and cyber attacks by more organized cyber criminal groups in the late 2000s. The country also became a global source of malware attacks [63]. Recognizing cybersecurity as a priority, the Bangladesh government has taken key cybersecurity initiatives over the years, including the establishment of BGD e-Gov CIRT in 2008 to address cyber threats, the amendment of the ICT Act in 2013 to criminalize cyber crimes, the adoption of the National Cyber Security Strategy in 2014 to strengthen capabilities, and the launch of BdCERT in 2021 for national incident response coordination. Despite these efforts, significant gaps in implementation and preparedness remain as the country's digital transformation progresses [63]. Bangladesh, like most countries, faces growing cybersecurity threats, particularly from botnet attacks that target critical sectors such as the government institutions, healthcare, and financial sectors. Several government bodies play a role in overseeing and implementing Bangladesh's cyber security measures. Bangladesh Computer Incident Response Team (BGD e-Gov CIRT) monitors cyber threats and coordinates incident responses, while the Bangladesh Telecommunica-

tion Regulatory Commission (BTRC) secures telecom networks and infrastructure. The Cyber Crime Unit of the CID investigates cyber crimes, and Bangladesh Bank handles cyber security in the banking and financial sector [63].

Bangladesh’s legal framework for cyber security includes:

1. The ICT Act 2006 (amended 2013), which criminalizes cyber crimes like hacking, data theft, and online defamation
2. The Bangladesh Computer Security Incident Response Team Regulation 2015, which outlines BGD e-Gov CIRT’s mandate
3. Bangladesh Bank also issued cyber security guidelines for banks and financial institutions in 2015.

Although the country has implemented a National Cybersecurity Strategy, the framework is largely outdated and insufficient to address the modern ever-growing cyber threats [39]. Several key gaps are as follows:

- Outdated cybersecurity laws and framework and the absence of mandatory training for senior policymakers hinders Bangladesh’s ability to effectively respond to cyber-threats.
- The country lacks comprehensive security standards for software which leaves users exposed to botnet infections and other malware.
- There is no formal involvement of the Armed Forces in national cybersecurity defense which reduces preparedness for large-scale cyberattacks.

Without the implementation of strong real-time detection tools and modernized processes, Bangladesh’s current framework seems to be only reactive rather than proactive.

## 10.2 Security Experts’ Recommendations: Focus on People, Process, and Technology

The security experts at Pipeline Inc. believe in a stronger approach to cybersecurity for Bangladesh. In order to build a comprehensive framework to tackle botnet attacks, the experts recommend focusing on three critical areas which are people, process and technology. This strategy ensures to build a more resilient defense against the growing threats posed by botnets and other cyberattacks in Bangladesh as it covers all angles.

### People

The general population of a country are the potential victims of the attackers. As highlighted in Chapter 5, one of the most significant vulnerabilities in Bangladesh’s cybersecurity landscape is the lack of awareness, education, and training among individuals of the general public. From the insights gained through this study’s analysis, it is found that human error is the leading factor in the spread of botnet infections.



This is primarily caused by insufficient knowledge of cyber threats and a lack of cyber hygiene. To mitigate this risk, security experts [37] recommend nationwide cyber-security awareness campaigns to educate both citizens and professionals about the dangers posed by botnets and the best practices in order to maintain digital hygiene.

As discussed in Chapter 6, 52.8% of the local botmasters use social engineering tactics, taking advantage of the public's lack of awareness. To fight this challenge, Bangladesh University of Professionals offers a BSc in Cyber Security and cyber defense courses, while the Military Institute of Science and Technology provides certification programs. Private institutes like Cyber Genius and DC Cyber offer specialized courses, and the government's "Skills for Employment Investment Program" focuses on cyber security skills development [63]. Therefore, more universities in Bangladesh should take the initiative to educate the future of the country on these pressing issues.

Besides public education on cybersecurity, mandatory cybersecurity training should be implemented for government officials, especially for those who are involved in critical decision-making roles. From the hypothesis testing done in Chapter 5, it is observed that awareness of botnets does not necessarily translate to best security practices. Therefore, mandatory training needs to be enforced in critical sectors along with strict policies that will check compliance to digital hygiene. This would ensure that key figures are equipped with the necessary knowledge to manage and mitigate cyber risks effectively. Fostering a culture of cybersecurity education from schools to professional settings would further embed a strong understanding of digital safety which will help reduce the likelihood of human error contributing to botnet attacks.

## Process

In Bangladesh's current cybersecurity framework, there is an absence of a well-defined process for detection and response to cyber incidents. Although the BGD e-GOV CIRT now operates 24/7, this gap can ultimately contribute to Bangladesh's downfall. Therefore, experts recommend to include more structured and efficient incident detection, mitigation, and post-attack procedures which will help establish clear forensic analysis. These protocols will ensure that cyberattacks are thoroughly investigated which allows for better prevention of future incidents. Moreover, mandatory audits and compliance checks across the critical sectors, such as financial and government are crucial to ensure that organizations adhere to national cybersecurity standards.

From the analysis done in Chapter 6, it is observed that local attackers mostly target government institutions. In addition, small businesses and large corporations are targeted for botnet inclusion. It is to be noted that cybersecurity is not solely the responsibility of the government. Collaboration between the government and private sectors is crucial to ensure a robust defense mechanism. In Bangladesh, 522 cybercrime incidents were reported to the government in 2022, reflecting a 40% decrease from the 875 incidents recorded in 2021. In 2023, only 185 cases were reported which indicates that the total figure for 2023 was significantly lower than previous

years [58]. Both private and public sectors need to address cyber incidents openly instead of hiding them. Gatekeeping only hinders progress and prevents others from truly assessing the situation. Every organization faces cyber attacks, it is inevitable. Therefore, instead of covering up, it is crucial that the incident reports are shared among the security experts to analyze which will ultimately help identify patterns, weaknesses, and solutions to protect the nation from future attacks. The private sector plays a crucial role in strengthening Bangladesh's cyber defenses. Major telecoms like Grameenphone and Robi have cyber security centers, while financial institutions like BRAC Bank invest in cyber security tools, ethical hacking, and training. Cyber security firms such as Sotenberg, Duaa, and SquareTech provide audits and incident response support. E-commerce companies like Chaldal focus on secure payments and data protection for customers [63]. By transparently sharing these incidents, Bangladesh can collectively work toward stronger defenses and benefit from the knowledge gained from these challenges.

## Technology

As seen in Chapter 6, most local attackers do not gather information on cybersecurity trends and they do not deploy sophisticated evasion tactics. As Bangladesh currently relies on reactive measures as opposed to proactive ones, security experts recommend implementing Intrusion Detection systems (IDS) and Intrusion Prevention Systems (IPS) for a multi-layered approach. By using open-source tools such as Snort for signature-based detection and Suricata for advanced and multi-threaded detection in high-traffic environments it is possible to improve detection precision as it is unlikely for local botmasters to opt for complex evasion techniques. Moreover, Host-based Intrusion Detection Systems (HIDS) such as OSSEC, can provide real-time log analysis, file integrity monitoring, and endpoint detection which adds another layer of defense. Furthermore, DNS filtering and centralized logging systems should be used to collect and analyze data for better forensic analysis. Additionally, automation tools like crontab and periodic tuning scripts can also help ensure that detection rules are regularly updated to keep up with evolving threats. By implementing these all together, it is possible to be protected from botnet inclusion. As highlighted in Chapter 6, local botmasters do not invest on infrastructure costs. Therefore, these tools can mitigate the risk of primitive botnet attacks.

## 10.3 Learning from Singapore: A Model for Bangladesh

Singapore's cybersecurity framework is highly regarded globally and consistently ranks among the top nations for cybersecurity preparedness. According to the Global Cybersecurity Index (GCI), Singapore is placed within the top ten globally for its comprehensive approach to tackling cyber threats [41]. The country has earned praise for its resilience in protecting critical sectors, proactive threat monitoring systems, and strong international cooperation efforts. This ranking highlights Singapore's up-to-date framework, driven by well-thought-out policies and consistent innovation.

Singapore’s Cybersecurity Strategy 2021 provides a model for building a resilient and proactive cybersecurity framework [42]. The strategy heavily focuses on protecting its Critical Information Infrastructure (CII) through continuous monitoring and strong regulatory frameworks. Bangladesh can draw inspiration from this strategy to extend protection to its critical sectors, which are frequently targeted by local botmasters. Singapore also integrates real-time monitoring systems powered by AI to enable early detection of cyber threats. Additionally, the strategy emphasizes international cooperation and talent development.

Therefore, the key strengths of the Singaporean cybersecurity framework are:

- **Resilient Infrastructure:** Focusing on critical structures through continuous monitoring and regulatory frameworks.
- **Proactive Threat Monitoring:** Integrating real-time threat monitoring systems with AI-powered tools for the benefit of early detection.
- **International Cooperation and Talent Development:** Building a robust cybersecurity talent pipeline and participating in global cybersecurity dialogues in order to learn.

## 10.4 Proposed Framework for Bangladesh: People, Process, and Technology

The following framework is constructed to make up for the gap in the current cybersecurity framework of Bangladesh, to protect against botnet attacks, incorporating elements and taking inspiration from both local security experts’ recommendations and Singapore’s cybersecurity strategy.

### 1. People

- **Mandatory Training and Awareness:** Develop a cybersecurity training curriculum for government officials and critical sector employees. In order to achieve this, the government can partner with cybersecurity firms and provide training at regular and appropriate intervals. This training should include modules on botnet threats, digital hygiene, and cyber incident response. Strict policies should be enforced, requiring employees to adhere to the training and digital hygiene. Their compliance should be regularly monitored and failing to follow the protocols should result in appropriate consequences to ensure consistent security standards.
- **Public Education Campaigns:** Launch awareness campaigns to educate citizens on the importance of cybersecurity. Promote secure online behaviors and inform them about the dangers of botnets. Moreover, advocate cybersecurity in universities by facilitating research.
- **Upskilling Programs and Creating Career Paths:** Establish cybersecurity boot camps and mentorship programs for youth and mid-career professionals to build a strong talent pool. As well as create career paths within the cybersecurity field to attract and retain talent.

## 2. Process

- **Collaboration Between Private and Public Sectors:** Collaboration among the public and private sectors is crucial for the security experts of the country to get a clear idea about the ever-growing cyber threat patterns, weaknesses in the system, and possible solutions. Therefore it is vital to report incidents in order to analyze and to share threat intelligence.
- **International Collaboration:** International collaboration will help security professionals of the nation to learn about new threats and ways to mitigate them as well as maintain international standards. This can be achieved through attending international security conferences or sharing insights with global cybersecurity firms.
- **Centralized Logging and Forensics:** Implement a centralized logging system that aggregates data from Snort, Suricata, and OSSEC for better correlation and forensic analysis of attacks.
- **Incident Response Protocols:** Define clear post-attack mitigation strategies to ensure rapid recovery from botnet infections and minimize downtime. In order to achieve this, the BGD e-Gov CIRT team must compile a protocol that will contain clear instructions for detection, containment, eradication, and recovery steps. This protocol must be tested through drills and be approved at a regular interval. The CIRT team should make adjustments as necessary.

## 3. Technology

- **Integration of IDS and IPS Tools:** Deploy Suricata as the primary IDS for high-traffic environments due to its multi-threading capabilities and Snort as the second layer for detecting known botnet signatures.
- **Integration of HIDS tools:** Use OSSEC for host-based intrusion detection, performing real-time log analysis and file integrity checks to protect individual systems.
- **Automated Rule Updates and Tuning:** Implement automated rule updates and tuning scripts to maintain up-to-date threat intelligence and detection accuracy, minimizing false positives.
- **DNS Filtering and Proactive Tools:** Introduce DNS filtering to block malicious traffic and integrate AI-driven threat-hunting tools to detect emerging threats in real-time.

Figure 10.1 illustrates the proposed framework for Bangladesh while focusing on people, process, and technology.

In conclusion, safeguarding Bangladesh from botnet threats requires focusing on people, process and technology. By spreading awareness and education on botnets, it is possible to mitigate human errors and mandatory training ensures that employees of critical sectors are safe from social engineering tactics employed by the local attackers. Moreover, by introducing upskilling programs and creating career paths, the government can ensure a talented pool and to attract and encourage

## Proposed Framework For Bangladesh

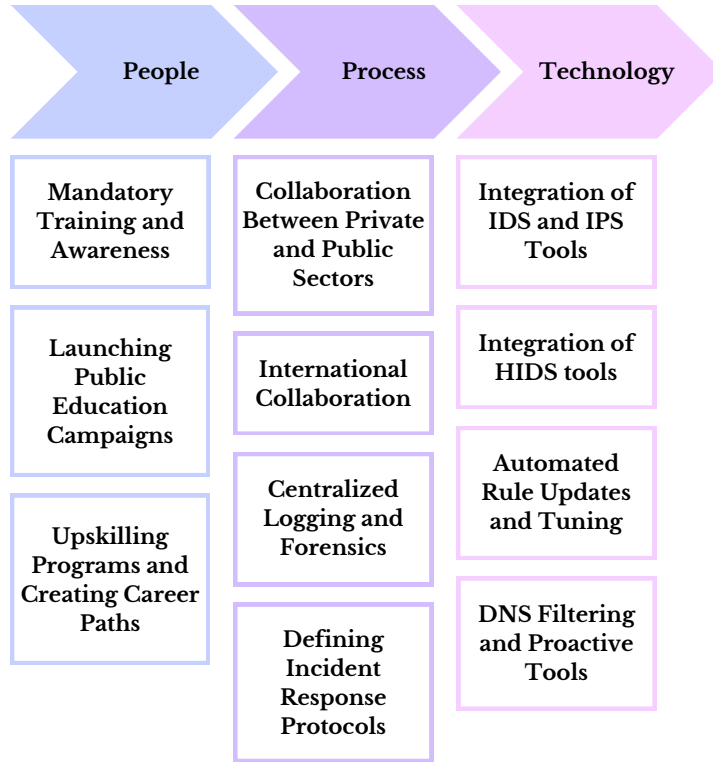


Figure 10.1: Proposed Framework For Bangladesh

enthusiastic individuals to pursue in cybersecurity fields. Moreover, implementing an integrated approach by combining the strengths of different IDS and HIDS solutions. By leveraging from the features of Snort and Suricata threat detection in real-time can be implemented and using OSSEC log and file analyzing. Hence reducing false positives, and performance enhance in high-traffic scenarios. Regular tuning, automated rule updates, and centralized logging will further improve the framework's resilience against the rapidly evolving botnet landscape. Moreover, in order to learn about ever-growing cyber threats like botnets, the government must ensure collaboration among the private and public sectors as well as on international grounds. Furthermore, it is necessary to define clear incident response protocols to prevent prolonged downtimes.

# Chapter 11

## Conclusion and Future work

As outlined, the objective of this research was to enhance Bangladesh's defensive framework to protect its digital landscape against botnet attacks and mitigate their economic impact. By addressing the concerns, this study explored the life-cycle of botnets, their economic consequences for the general public and businesses, and the underlying motivations of attackers. The study provides valuable insights in understanding the cybersecurity vulnerabilities specific to Bangladesh's crucial sectors. This is gained through Exploratory Data Analysis (EDA) and expert interviews while highlighting the need for enhanced detection and mitigation strategies.

The key findings of this research revealed several important insights. From the general public's perspective, a lack of awareness and vulnerability towards social engineering significantly increases the risk of botnet attacks. The public's failure to update software and recognize suspicious activity also contributes to the spread of botnets. From the attackers' perspective, botnet operators in Bangladesh focus on local, high-value targets, leveraging financial incentives like trojan attacks, and using social engineering techniques such as phishing to propagate. Moreover, local botmasters use anonymous services, and encrypted protocols to evade detection. Furthermore, the interview with security experts highlighted key indicators of botnet infections, such as unusual outbound traffic and devices communicating with suspicious IP addresses. They also stressed ongoing challenges, particularly with botnets' evolving nature, which complicates detection efforts, and the reluctance to report incidents due to privacy concerns.

The proposed framework developed through this research is highly relevant for the financial sector, helping to prevent significant economic losses by improving detection capabilities and promoting proactive cybersecurity measures. This was accomplished by performing a technical analysis on open-source Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) such as Suricata and Snort which demonstrated their effectiveness in identifying botnet activities, making them crucial for sectors needing free-of-cost but efficient cybersecurity solutions. However, a major limitation of this research was the inability to obtain data from Bangladeshi financial institutions due to their concerns about reputational damage. This reflects a larger issue in the cybersecurity field within Bangladesh, where the lack of transparency and incident reporting hinders collective defensive efforts.

In conclusion, this research emphasizes the importance of strengthening Bangladesh's cybersecurity framework. It also offers valuable insights to protect Bangladesh's digital assets from the growing threat of botnets by providing technical solutions and recommendations of strategies. Facing cyber attacks is inevitable in this digital world. Therefore, it is necessary to be prepared for such attacks and to acknowledge weaknesses. Otherwise it will be quite difficult to adapt to this modern cyber landscape. The framework proposed in this research is not far fetched and impossible to implement. It is high time the people of Bangladesh acknowledge the loopholes and vulnerabilities in its system and take accountability before another 2016 Bank heist or a Nagad data leak occurs. Therefore, it is crucial for Bangladesh to implement the proposed cybersecurity framework outlined in this research. By doing so, the nation can address the existing gaps in its cybersecurity posture and fortify its defenses against botnet attacks.

## **Objective Analysis:**

An objective analysis for this research work is as follows-

- Understanding the botnet life-cycle from its initial infection to retirement - this has been discussed in detail in Chapter 2 Background. In order to achieve the first objective, numerous previous papers have been read. From those studies, the entire life cycle of a botnet was constructed part-by-part for a comprehensive section of this research.
- Exploring the reasons or motivations behind botnet attacks by analyzing the attacker's perspective - it has been elaborated in Chapter 6 Attacker's Perspective. Unlike the method chosen for the first objective, an online survey was carried out to be able to obtain local attackers' data for an in-depth analysis to explore their inspiration for carrying on with destructive botnet attacks. As a result of the survey, it was possible to gather 46 Bangladeshi hackers' information which assisted in surfacing important trends. Therefore, the acquired data's qualitative value is much higher which helps in ultimately revealing the bigger picture through this study.
- Investigating the economic impacts of botnets on the financial sectors in Bangladesh - the findings have been described in Chapter 5 Victim's Perspective, Chapter 7 Security Expert's Perspective, & Chapter 8 Analysis & Discussion. Similar to the second one, this third objective was also accomplished through a survey from a general mass viewpoint as well as a semi-structured interview, and extensive analysis of the garnered data. A brief overview on how the third objective of gaining insight on economic impacts was achieved would be the thorough data analysis of the collected data from the general population, and information gotten from the interviewed security professionals.
- Assessing the challenges and effectiveness of current detection and mitigation efforts that are put in place by cybersecurity agencies, while also evaluating existing mitigation tools, strategies and identifying prevention measures to minimize the economic impact of botnets in Bangladesh-the related intricate discoveries are illustrated in Chapter 9 Technical Evaluation. Contrary to the

initial three objectives, this fourth one was executed via technical assessment of existing open-source cybersecurity tools such as Snort, Suricata and OSSEC. They were evaluated through multiple attacking experiments to reveal their effectiveness and difficulty in prevention and detection methods, to eventually be able to shut off the financial blow due to botnet attacks.

- Establishing a comprehensive defensive framework for Bangladesh against botnets - relevant revelations have been presented in Chapter 10 Proposed Framework for Bangladesh. Finally, coming to the fifth and last objective which is the proposal of a cybersecurity framework specifically tailored for Bangladesh to defend itself against botnet attacks. To put together the defensive framework, three things were given the utmost importance- people, process, and technology. Here, people means human beings should be given a minimum formal training on how to enforce security and not fall for social engineering tactics, etc. Additionally, process refers to cross-collaboration in terms of security of different sectors whether national and international, reporting security breach incidents, etc. Lastly, the technology part includes the usage of IDS, IPS, and HIDS along with DNS filtering to keep out such botnet attacks from the virtual borders of Bangladesh.

Therefore, the objective analysis for all five objectives of this research has been reviewed above.

## **Future Work**

Future research could focus on extending the framework by optimizing botnet detection tools, considering the pros and cons highlighted in this research's technical evaluation. This would enhance their ability to detect evolving threats in real-time, making them more adaptable to the changing landscape of cyber threats. Developing cohesive cybersecurity policies and encouraging information sharing can improve overall security measures in Bangladesh. Exploring the development of intrusion detection systems for smaller form factor devices such as IoT devices can also be useful for preventing cyber threats such as botnets intrusion. Devices such as smart cameras, digital thermostats, sensors, and other consumer gadgets could be equipped with Snort and Suricata or similar IDS tools that are good for lower resource usage. This would enable real-time detection of malicious traffic and threats on smaller devices without the need for resource-intensive PCs that are running heavy OS like Windows or Ubuntu. This would allow for more distributed security mechanisms reducing the reliance on centralized systems and improving the overall strength of the network the devices are in. The adaptability and cost efficiency of this approach could greatly enhance cybersecurity across various sectors such as industries, banks, and healthcare and in environments where full-scale IDS is not very feasible.

Hence, this would enable more effective threat intelligence and collective responses to botnet attacks. By refining both technical tools and promoting collaborative cybersecurity efforts, the economic burden of these malicious activities caused by botnets can be significantly reduced. Future work can contribute by creating a more secure and resilient digital ecosystem in Bangladesh.



# Bibliography

- [1] D. Georgoulas, A. Dimitrios, D. Andronikos, and P. Papadimitriou, “Botnet business models, take-down attempts, and the darkweb market: A survey,” *\*ACM Computing Surveys\**, vol. 55, no. 11, pp. 1-39, 2023.
- [2] H. Tiirmaa-Klaar, J. Gassen, E. Gerhards-Padilla, and P. Martini, “Botnets: How to fight the ever-growing threat on a technical level,” *\*Botnets\**, pp. 41-97, 2013.
- [3] C. G. J. Putman and L. J. M. Nieuwenhuis, “Business model of a botnet,” in *\*2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)\**, IEEE, 2018, pp. 1-6.
- [4] B. Stone-Gross, T. Holz, G. Stringhini, and G. Vigna, “The underground economy of spam: A botmaster’s perspective of coordinating large-scale spam campaigns,” in *\*4th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET 11)\**, 2011.
- [5] M. A. Hossain and M. Hasan, “A simplified cybersecurity policy framework for the financial institutions in Bangladesh: A survey of literature,” *\*DUJST\**, vol. 42, no. 3, pp. 41-81, 2023, doi: 10.3329/dujbst.v42i3.65120.
- [6] Government of Bangladesh, “Bangladesh cyber threat landscape 2022,” ICT Division, 2022. [Online]. Available: [https://ictd.gov.bd/sites/default/files/files/ictd.portal.gov.bd/publications/effc311d\\_5097\\_46ba\\_afa4\\_5f44b60a93e6/Bangladesh%20Cyber%20Threat%20Landscape%202022.pdf](https://ictd.gov.bd/sites/default/files/files/ictd.portal.gov.bd/publications/effc311d_5097_46ba_afa4_5f44b60a93e6/Bangladesh%20Cyber%20Threat%20Landscape%202022.pdf). [Accessed: Oct. 11, 2024].
- [7] Deloitte, “RBI guidelines for cyber security framework,” Deloitte, July 2016. [Online]. Available: <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-rbi-guidelines-for-cyber-security-framework-noexp.pdf>. [Accessed: Oct. 11, 2024].
- [8] N. Hachem, Y. B. Mustapha, G. G. Granadillo, and H. Debar, “Botnets: life-cycle and taxonomy,” in *2011 Conference on Network and Information Systems Security*, IEEE, May 2011, pp. 1–8.
- [9] J. Yadav and J. Thakur, “Botnet: Evolution life cycle architecture and detection techniques,” *\*Mukt Shabd Journal\**, vol. 9, no. 6, pp. 4265-4281, 2020.
- [10] M. S. Sonawane, “A survey of botnet and botnet detection methods,” *\*International Journal of Engineering Research & Technology (IJERT)\**, vol. 7, no. 12, 2018.

- [11] R. A. Rodríguez-Gómez, G. Maciá-Fernández, and P. Garcia-Teodoro, “Analysis of botnets through life-cycle,” in Proceedings of the International Conference on Security and Cryptography, IEEE, 2011, pp. 257–262.
- [12] M. Sully and M. Thompson, “The deconstruction of the Mariposa botnet,” \*Defence Intelligence\*, Sep. 16, 2010.
- [13] The Economic Times, “India sees sharp increase in cyberattacks in Q1 2023: Report,” \*The Economic Times\*, May 9, 2023. [Online]. Available: <https://economictimes.indiatimes.com/tech/technology/sharp-increase-in-cyberattacks-in-india-in-q1-2023-report/articleshow/100096450.cms>. Accessed: Oct. 11, 2024.
- [14] World Economic Forum, “Cybersecurity: Governments and business,” \*World Economic Forum\*, May 5, 2021. Accessed: May 24, 2024.
- [15] F. Salahdine and N. Kaabouch, “Social engineering attacks: A survey,” \*Future Internet\*, vol. 11, no. 4, p. 89, 2019.
- [16] A. Bowker, \*The Cybercrime Handbook for Community Corrections: Managing Offender Risk in the 21st Century\*, Charles C Thomas Publisher, 2012.
- [17] D. S. Wall, \*Cybercrime: The Transformation of Crime in the Information Age\*, John Wiley & Sons, 2024.
- [18] L. F. Cranor and S. Garfinkel, \*Security and Usability: Designing Secure Systems that People Can Use\*, O’Reilly Media, Inc., 2005.
- [19] R. Dhamija, J. D. Tygar, and M. Hearst, “Why phishing works,” in \*Proceedings of the SIGCHI Conference on Human Factors in Computing Systems\*, 2006, pp. 581-590.
- [20] E. J. Kartaltepe, J. A. Morales, S. Xu, and R. Sandhu, “Social network-based botnet command-and-control: Emerging threats and countermeasures,” in \*Applied Cryptography and Network Security: 8th International Conference\*, Beijing, China, Jun. 22-25, 2010, vol. 8, pp. 511-528.
- [21] Broadcom, \*Internet Security Threat Report Volume 22\*, Broadcom, 2017. [Online]. Available: <https://docs.broadcom.com/doc/istr-22-2017-en>. Accessed: May 24, 2024.
- [22] M. E. Whitman and H. J. Mattord, \*Principles of Information Security\*, Boston, MA: Thomson Course Technology, 2009.
- [23] C. H. Malin, E. Casey, and J. M. Aquilina, \*Malware Forensics Field Guide for Windows Systems\*, Syngress, 2012.
- [24] D. Stuttard and M. Pinto, \*The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws\*, John Wiley & Sons, 2011.
- [25] C. Hadnagy, \*Social Engineering: The Art of Human Hacking\*, John Wiley & Sons, 2010.

- [26] J. Hariharan, A. T. Sheik, C. Maple, N. Beech, and U. I. Atmaca, "Customers' perception of cybersecurity risks in e-commerce websites," in *\*International Conference on AI and the Digital Economy (CADE 2023)\**, IET, 2023, pp. 53-60.
- [27] C. Gersch and J. Birkett, "Password security: A research paper," [Online]. Available: <https://cyberhound.com/wp-content/uploads/CH-Research-Paper-Password-Security-LR-.pdf>. Accessed: May 24, 2024.
- [28] S. A. Taher and M. Tsuji, "An overview of FinTech in Bangladesh: Problems and prospects," in *\*FinTech Development for Financial Inclusiveness\**, 2022.
- [29] M. J. Hossain, R. H. Rifat, M. H. Mugdho, M. Jahan, A. A. Rasel, and M. A. Rahman, "Cyber threats and scams in FinTech organizations: A brief overview of financial fraud cases, future challenges, and recommended solutions in Bangladesh," in *\*2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)\**, IEEE, Jakarta, Indonesia, 2022, pp. 190-195.
- [30] M. A. Hossain, M. D. Sarker, M. S. Hossain, M. A. Shaon, M. S. Hossain, M. M. Rayhan, and J. G. Sepulveda, "Bangladesh Bank Money Heist: A concern of cybersecurity system of Bangladesh Bank and way forward," 2024.
- [31] S. Quadir, "Bangladesh bank says hackers tried to steal \$951 million," *\*Reuters\**, 2016.
- [32] Z. Islam, "Some user info of Nagad, other entities in public domain," *\*The Daily Star\**, 2024. Accessed: Oct. 11, 2024. [Online]. Available: <https://www.thedailystar.net/news/bangladesh/news/some-user-info-nagad-other-entities-public-domain-3564666>.
- [33] Bederna, Zsolt, and Tamas Szadeczky. "Cyber espionage through Botnets." *Security Journal* 33.1 (2020): 43-62.
- [34] Musiał, Nikoleta. "Cyber risk in financial institutions: A Polish case." *Multiple Perspectives in Risk and Risk Management: ERRN 8th European Risk Conference 2018*, Katowice, Poland, September 20-21. Springer International Publishing, 2019.
- [35] Das, B., Roy, J., Purkaystha, S., Ahmed, T., & Molla, M. S. *Cryptocurrency: Its Evolution, Transformative Future and Implications in Bangladesh*.
- [36] Aldawood, Hussain, and Geoffrey Skinner. "Educating and raising awareness on cyber security social engineering: A literature review." *2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE)*. IEEE, 2018.
- [37] M. M. Islam and A. S. M. S. Reza, Pipeline, personal communication, interviewed on July 1, 2024.
- [38] N. Clarke, S. Furnell, G. Tjhai, and M. Papadaki, "Investigating the problem of IDS false alarms: An experimental study using Snort," *International Federation*

- for Information Processing Digital Library; Proceedings of the IFIP TC 11 23rd International Information Security Conference, vol. 278, Jul. 2008, doi: 10.1007/978-0-387-09699-5\_17.
- [39] Uddin, Md Riaz. “The National Cybersecurity Strategy of Bangladesh: A Critical Analysis.” (2017): 12.
- [40] J. White, T. Fitsimmons, and J. Matthews, “Quantitative Analysis of Intrusion Detection Systems: Snort and Suricata,” in Proceedings of SPIE - The International Society for Optical Engineering, vol. 8757, Apr. 2013, doi: 10.1117/12.2015616.
- [41] “Singapore Ranks 10th in Global Cybersecurity Study.” Singapore Business Review, 19 May 2023, <https://sbr.com.sg/information-technology/news/singapore-ranks-10th-in-global-cybersecurity-study>. Accessed 13 Oct. 2024.
- [42] “Singapore Cybersecurity Strategy 2021.” Cyber Security Agency of Singapore, 2021, <https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021>. Accessed 13 Oct. 2024.
- [43] United News of Bangladesh, “Nagad becomes Bangladesh’s fastest unicorn,” United News of Bangladesh, July 29, 2023. [Online]. Available: <https://www.tbsnews.net/bangladesh/nagad-becomes-bangladeshs-fastest-unicorn-673442>. Accessed: 2024-10-14.
- [44] D. Day and B. Burns, “A performance analysis of Snort and Suricata network intrusion detection and prevention engines,” in \*Proceedings of the 2011 Cybersecurity Conference\*, Feb. 2011, pp. 1-8.
- [45] Bederna, Zsolt, and Tamás Szádeczky. “Effects of botnets—a human-organisational approach.” Security and Defence Quarterly 35 (2021).
- [46] Vladimir Unterfingher. A Technical Analysis of the Mirai Botnet Phenomenon: Mirai Botnet Attack and Infection Methodologies. Heimdal Security. Last updated on February 10, 2023. Available at: <https://heimdalsecurity.com/blog/mirai-botnet-phenomenon/> (Accessed: 2024-10-15).
- [47] Haner, Justin K., and Robert K. Knake. “Breaking botnets: A quantitative analysis of individual, technical, isolationist, and multilateral approaches to cybersecurity.” Journal of cybersecurity 7.1 (2021): tyab003.
- [48] Maalem Lahcen, Rachid Ait, et al. “Review and insight on the behavioral aspects of cybersecurity.” Cybersecurity 3 (2020): 1-18.
- [49] B. Stephens, A. Shaghghi, R. Doss, and S. S. Kanhere, “Detecting internet of things bots: A comparative study,” IEEE Access, vol. 9, pp. 160391–160401, 2021.
- [50] Babu, K. E. K. “Cyber Security in the Global Village and Challenges for Bangladesh: An Overview on Legal Context.” Cybersecurity, Privacy and Freedom Protection in the Connected World (2021): 253-267.

- [51] Dupont, Benoit. “Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cyber-crime.” *Crime, law and social change* 67 (2017): 97-116.
- [52] Othman, Suad Mohammed and Alsohybe, Nabeel T and Ba-Alwi, Fadl Muta-her and Zahary, Ammar Thabit, Survey on intrusion detection system types, *International Journal of Cyber Security and Digital Forensics*, vol. 7, no. 4, pp. 444–463, 2018. The Society of Digital Information and Wireless Communica-tions.
- [53] D. Teixeira, L. Assunção, T. Pereira, S. Malta, and P. Pinto, “OSSEC IDS extension to improve log analysis and override false positive or negative detec-tions,” *\*Journal of Sensor and Actuator Networks\**, vol. 8, no. 3, p. 46, 2019.
- [54] Pentescop. “Understanding Botnets: How to Detect and Defend Against Them.” Pentescop, <https://pentescop.com/understanding-botnets-how-to-detect-and-defend-against-them/>. Accessed 16 Oct. 2024.
- [55] “Information Gathering in Cyber Security.” Scaler, Scaler Academy, [www.scaler.com/topics/cyber-security/information-gathering-in-cyber-security/](http://www.scaler.com/topics/cyber-security/information-gathering-in-cyber-security/).
- [56] I. Mukhopadhyay, M. Chakraborty, and S. Chakrabarti, “A comparative study of related technologies of intrusion detection & prevention systems,” *J. Informa-tion Security*, vol. 2, pp. 28-38, Jan. 2011, doi: 10.4236/jis.2011.21003.
- [57] Bischoff, Paul. “Cybercrime Victims Lose an Estimated \$714 Billion Annually.” Comparitech, 5 Dec. 2023, [www.comparitech.com/blog/vpn-privacy/cybercrime-cost](http://www.comparitech.com/blog/vpn-privacy/cybercrime-cost).
- [58] McCart, Craig. “15+ Shocking Botnet Statistics.” Comparitech, 31 Oct. 2022, [www.comparitech.com/blog/information-security/botnet-statistics/](http://www.comparitech.com/blog/information-security/botnet-statistics/).
- [59] DemandSage. “Internet User Statistics.” DemandSage, 2024, [www.demandsage.com/internet-user-statistics](http://www.demandsage.com/internet-user-statistics).
- [60] CompTIA. “Cybersecurity Statistics and Facts.” CompTIA, 2024, <https://connect.comptia.org/blog/cyber-security-stats-facts>.
- [61] MacColl, Jamie, et al. “Ransomware: Victim Insights on Harms to Individuals, Organisations and Society.” (2024).
- [62] “The Cyphere. Malware Statistics to Be Taken Seriously in 2023.” The Cyphere, 2023, <https://thecyphere.com/blog/malware-statistics/>.
- [63] MeghOps. “What Is the Cyber Security Status of Bangladesh?” MeghOps, 7 May 2024, <https://blog.meghops.io/what-is-the-cyber-security-status-of-bangladesh>.

# Appendix 1

## Survey Questions

### General public's Survey

1. What is your age?
2. What is your current profession?
3. How much time do you spend on the internet each day?
4. What device do you use most often to access the internet?
5. What type of internet connection do you use the most?
6. How many years have you been using internet-connected devices (e.g., computers, smartphones)?
7. Have you received any education or training on cybersecurity topics, including botnets?
8. How familiar are you with botnets?
9. Have you ever experienced any of the following issues with your devices? (Select all that apply)
10. How often do you update the software and firmware on your devices?
11. How often do you seek information about cybersecurity threats and best practices?
12. If you suspect your device is infected with malware, what would you do?
13. Do you believe your devices are secure from cyber threats such as botnets?
14. How much would you be willing to pay to protect against botnet attacks?
15. How often do you change your passwords?
16. How often do you click on links or download attachments from unknown sources?
17. Do you download cracked software or games (obtained illegally without proper licensing)?

18. Have you ever experienced a cybersecurity incident (e.g., malware infection, phishing attack)?
19. Does the idea of a potential botnet attack cause you any stress or anxiety?
20. Does the fear of botnet attacks influence your trust in online platforms and e-commerce?

## **Attackers Survey**

1. How do you stay updated on all aspects of cybersecurity relevant to botnet operations? (Select all that apply)
2. What methods do you use to identify high-value targets suitable for inclusion in your botnet? (Select all that apply)
3. Have you encountered any countermeasures or defensive strategies employed by potential targets that have significantly hindered your botnet activities?
4. What are the main objectives or purposes for which you deploy botnets in your operations? (Select all that apply)
5. Which South Asian countries do you commonly target? (Select all that apply)
6. Do you primarily target:
7. How do you primarily monetize your botnet activities?
8. What factors influence the revenue generated from your botnet operations? (Select all that apply)
9. What are the primary costs associated with maintaining and operating your botnet? (Select all that apply)
10. How do you measure the success and profitability of your botnet operations?
11. Approximately, how much money do you estimate you earn from your botnet activities each month?
12. How do you handle financial transactions related to your botnet activities?
13. What legal and regulatory risks do you encounter in conducting botnet operations?
14. What factors typically influence the decision to retire a botnet operation?
15. How do you ensure the scalability and adaptability of your botnet infrastructure to accommodate growth and changing requirements?
16. How do you initially compromise devices to establish control over them for botnet deployment?
17. Once control over a device is established, how do you propagate the botnet to additional devices?

18. How do you set up and maintain the command and control infrastructure for your botnet?
19. What techniques do you employ to evade detection by security measures or antivirus software during deployment? (Select all that apply)
20. How do you adjust tactics in response to evolving security measures and target countermeasures against botnet activities?
21. How do you select targets for inclusion in your botnet operations?
22. How do you mitigate the risk of botnet takedowns or disruptions by law enforcement or cybersecurity agencies?
23. What methods do you use to communicate covertly with devices within your botnet? (Select all that apply)
24. Once you gain control over a device or include it in your botnet, what are the primary activities you perform with the compromised device?
25. How do you issue commands to devices within your botnet to carry out specific tasks or activities?
26. What measures do you take to maintain and manage devices within your botnet over time? (Select all that apply)



# Appendix 2

## Glossary

- Botmaster: The individual who controls a botnet and issues commands towards infected devices to perform certain activities.
- Botnet: A network of devices, infected with malicious software and are controlled by a botmaster to perform malicious tasks.
- C&C (Command and Control) Server: The central server used by the botmaster to issue command and communicate with the infected devices.
- Zombie: An infected device which performs activities without the owners knowledge.
- DDoS (Distributed Denial of Service): A type of attack which floods a target server with overwhelming number of traffic.
- Polymorphism: A technique used by malware's to change their behaviour on each execution to avoid being detected.
- IP Spoofing: Method to send data packets using forged IP address to mask identity of the attacker.
- Botnet-as-a-Service (BaaS): A business model where cybercriminals rent out botnets to attackers for malicious intent.
- Cryptomining: Using computing resources to mine cryptocurrency.
- Sinkhole: A server used to capture and analyze malicious traffic, in an attempt to identify botnet and take it down by redirecting its communication.
- Trojan: A type of malware disguised as a legitimate software that once executed allows unauthorized access or control of the system.
- IRC (Internet Relay Chat): A protocol for real-time text communication over the internet through channels or via private messages.
- Fast-flux Networks: A technique that is used by botnets to hide phishing and malware delivery sites behind constantly changing IP addresses.
- SQL Injection: Manipulating SQL queries to throw error messages and reading unauthorized data from the database exploiting web vulnerabilities.

- Zero-day Exploit: A form of cyber attack targeting a software vulnerability before the author of the software or the vendor has patched it.
- Metamorphic Malware: Malware that can alter its code while maintaining its functionality in order to evade being detected.
- Social Engineering: A form of tactic which manipulates people into performing certain actions.
- Cryptography: A method of ciphering texts that only authorized parties can decipher.
- LSASS Vulnerability: A fatal flaw in the Local Security Authority Subsystem Service (LSASS) which can be exploited to steal credentials or gain unauthorized access to system.
- Emotet: A complex strain of malware which can steal personal information and spam a system with malicious emails or install more malware's on the infected system.
- Instant Messaging Worms: Bot binary that spreads through instant messaging platforms which is often done by tricking users into clicking infected links.
- Secondary Injection: Malicious payloads that are delivered after an initial compromise or infection of a system.
- Ciphering: The process of encoding data using some logic's to protect its confidentiality.
- Drive-by Downloads: Unintentionally downloads of malware which are often done by visiting malicious websites or clicking of malicious links.
- Attack Vectors: Methods that attacker uses or exploits to infiltrate a system and perform malicious activities.