Darknet as a Source of Cyber Threat Intelligence: Investigating Distributed and Reflection Denial of Service Attacks

Claude Fachkha

A Thesis
in
The Department
of
Electrical and Computer Engineering

Presented in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy at
Concordia University
Montreal, Quebec, Canada

November 2015

CONCORDIA UNIVERSITY
SCHOOL OF GRADUATE STUDIES

This is to certify that the thesis prepared

By: **Claude Fachkha**

Entitled: **Darknet as a Source of Cyber Threat Intelligence: Investigating Distributed and Reflection Denial of Service Attacks**

and submitted in partial fulfilment of the requirements for the degree of

Doctor of Philosophy

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

Dr. Deborah Dysart-Gale Chair
Dr. Mohammad Zulkernine External Examiner
Dr. Joey Paquet External to Program
Dr. Rachida Dssouli Examiner
Dr. Roch H. Glitho Examiner
Dr. Mourad Debbabi Thesis Supervisor

Approved by

Dr. Abdel Razik Sebak
Chair of Department or Graduate Program Director

Dr. Amir Asif
Dean of Faculty

ABSTRACT

Cyberspace has become a massive battlefield between computer criminals and computer security experts. In addition, large-scale cyber attacks have enormously matured and became capable to generate, in a prompt manner, significant interruptions and damage to Internet resources and infrastructure. Denial of Service (DoS) attacks are perhaps the most prominent and severe types of such large-scale cyber attacks. Furthermore, the existence of widely available encryption and anonymity techniques greatly increases the difficulty of the surveillance and investigation of cyber attacks. In this context, the availability of relevant cyber monitoring is of paramount importance. An effective approach to gather DoS cyber intelligence is to collect and analyze traffic destined to allocated, routable, yet unused Internet address space known as darknet. In this thesis, we leverage big darknet data to generate insights on various DoS events, namely, Distributed DoS (DDoS) and Distributed Reflection DoS (DRDoS) activities. First, we present a comprehensive survey of darknet. We primarily define and characterize darknet and indicate its alternative names. We further list other trap-based monitoring systems and compare them to darknet. In addition, we provide a taxonomy in relation to darknet technologies and identify research gaps that are related to three main darknet categories: deployment, traffic analysis, and visualization. Second, we characterize darknet data. Such information could generate indicators of cyber threat activity as well as provide in-depth understanding of the nature of its traffic. Particularly, we analyze darknet packets distribution, its used transport, network and application layer protocols and pinpoint its resolved domain names. Furthermore, we identify its IP classes and destination ports as well as geo-locate its source countries. We further investigate darknet-triggered threats. The aim is to explore darknet inferred threats and categorize their severities. Finally, we contribute by exploring the inter-correlation of such threats, by applying association rule mining techniques, to build threat association rules. Specifically, we generate clusters of threats that co-occur targeting a specific victim. Third, we propose a DDoS inference and forecasting model that aims at providing insights to organizations, security operators and emergency response teams during and after a DDoS attack. Specifically, this work strives to predict, within minutes, the attacks' features, namely, intensity/rate (packets/sec) and size (estimated number of compromised machines/bots). The goal is to understand the future short-term trend of the ongoing DDoS attacks in terms of those features and thus provide the capability to recognize the current as well as future similar situations and hence appropriately respond to the threat. Further, our work aims at investigating DDoS campaigns by proposing a clustering approach to infer various victims targeted by the same campaign and predicting related features. To achieve our goal, our proposed approach leverages a number of time series and fluctuation analysis techniques, statistical methods and forecasting approaches. Fourth, we propose a novel approach to infer and characterize Internet-scale DRDoS attacks by leveraging the darknet space. Complementary to the pioneer work on inferring DDoS activities using darknet, this work shows that we can extract DoS activities without relying on backscattered analysis. The aim of this work is to extract cyber security intelligence related to DRDoS activities such as intensity, rate and geo-location in addition to various network-layer and flow-based insights. To achieve this task, the proposed approach exploits certain DDoS parameters to detect the attacks and the expectation maximization and k-means clustering techniques in an attempt to identify campaigns of DRDoS attacks. Finally, we conclude this work by providing some discussions and pinpointing some future work.

DEDICATION

I dedicate this thesis to my parents, Antonio and Georgette, my brothers Jean and Gilbert, and my sister Nathalie. Thank you for your unconditional support with my studies. I am honored to be a member of your peaceful and lovely family. Thanks for standing by me and giving me an ever-lasting chance to prove and improve myself through all my walks of life. I love you all.

ACKNOWLEDGEMENTS

- I would primarily like to express my gratitude to my academic father and supervisor, Professor Mourad Debbabi, for the training and guidance during my graduate studies. Thanks for giving me the chance to work and grow with you. Furthermore, thanks for teaching me on perfectionism and dedication in the workplace throughout your professionalism and distinguished leadership skills.

- I thank National Cyber-Forensics & Training Alliance (NCFTA) Canada for providing facilities for conducting research, this work would not be possible without their active supports. I thank Farsight Security, Inc. and in particular, Dr. Paul Vixie, for access to rich data feeds.

- I would also like to express my appreciation towards the students, faculty and staff of Concordia University. I thank them for providing crucial aid and constant support throughout my graduate studies at Concordia University.

- I wish to extend my utmost gratitude to all my lab-mates and friends for their wonderful participation and cooperation. In particular, I would like to thank my friend, colleague and teammate, Dr. Elias Bou-Harb, who acted as a real brother during my PhD studies.

- Furthermore, I would like to thank my partner Flora for being so kind and loving.

- Last but not least, I would like to thank God, the natural power of creation, for giving me strength, courage, dedication, determination, patience, as well as guidance in conducting this long research study, despite all difficulties.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

Introduction

Today, the safety and security of our society are entirely dependent on having a secure Information Communication Technology (ICT) infrastructure, which spans over public and private organizations in the sectors of government, defense, energy (i.e., Nuclear and Power), telecommunications (i.e., mobiles), public health (i.e., hospitals), emergency services (i.e., 911), agriculture, finance (i.e., banks) and transportation (i.e., aviation). This infrastructure is controlled and operated using the Internet (also known as cyberspace): a network of numerous inter-connected computers.

Recent Internet events have demonstrated that corporations and governmental organizations could be subjected, nearly instantaneously and in full anonymity, to large-scale disrupting cyber attacks with the potential to lead to severe privacy, security and economic consequences (i.e., cyber terrorism, denial of service, information theft, spam, fraud, etc.). For instance, a nuclear power plant was targeted for the first time by Stuxnet, a complex computer virus discovered in 2010 [3]. In 2012, a more complicated malware known as Flame [4] was found to have massive espionage capabilities. There has been an increasing trend of cyber attacks, which have been used to exhaust and/or deny services of large organizations (.i.e., Google, Facebook, Government Websites) through the flood of computer network traffic to the victim targeted by the attack. For example, in 2014, the Internet experienced the largest DoS threat in history with 400 Gbps of bandwidth [5]. In addition, orchestrated cyber campaigns, which occur when a given cyber force conducts a series of planned and coordinated cyber attacks, leverage botnet (networks of orchestrated and infected computers) to communicate and execute attacks; such threats have caused over $110 billion in losses worldwide [6]. These events constitute a serious threat with the potential to endanger human lives, especially when physical entities such as smart grids [7] and nuclear power plants can be reached through cyberspace. The existence of widely available encryption and anonymity techniques greatly increases the difficulty of the surveillance and investigation of cyber attacks. In this context, the availability of relevant cyber monitoring is of paramount importance.

One of the effective ways to observe Internet activity is to employ passive monitoring using sensors or traps such as darknet [8]. Darknet data is defined as traffic targeting advertised, but unused, IP addresses. Since these network addresses are unused, they represent new hosts that have never been communicating with other devices, neither for benign or legitimate communication. As a result, any observed traffic destined to these non-interactive hosts raises suspicion and hence necessitates investigation. These darknet-based monitoring systems are designed through these unused IP addresses to attract or trap attackers for intelligence gathering. For instance, darknet has been used in the past to extract insights on: 1) probes or scanning activities [9] due to worms, bots and other automated exploit tools; 2) DDoS attacks due to victims' reply (backscatter) packets to spoofed IP addresses [10]; and 3) other activities, such as misconfiguration [1], and political events [11]. Darknet is an asset for network security. Several deployment techniques [12] were invented, various projects (i.e., CAIDA[1]) were built, and numerous visualization techniques were used in order to observe the data.

[1] The UCSD Network Telescope: `http://www.caida.org/projects/network_telescope/`

Denial of Service is an attempt to make a computer or network resources unavailable. It consists of attacks that are deployed to temporarily or indefinitely shutdown services. The timing of such attacks can be coordinated to exploit the availability of critical organization infrastructures by directing an enormous flood of Internet traffic towards targeted Internet Protocol (IP) addresses. By flooding the available bandwidth with intensive traffic, DDoS can effectively bring down a service with potential loss of brand name, trust, and financial revenue. Indeed, DoS activities continue to dominate today's attack landscape. In a recent report by Arbor Networks [13], it was concluded that 48% of all cyber threats are DoS. Furthermore, it was stated that the top 4 perceived threats for the next 12 months will be DDoS related, targeting customers, network and service infrastructures [14]. Some governmental organizations, corporations as well as ICT infrastructures were also recently deemed as DDoS victims [15–17]. Moreover, a recent event demonstrated that one of the largest cyber security organizations, namely Spamhaus, became a victim of a 300 Gbps Domain Name System (DNS) DDoS attack [18]. In addition to this, in 2014, the Internet has experienced the largest reflection DDoS attack in history [5]. Thus, DDoS attacks are a significant cyber security problem, causing momentous damage to several victims as well as negatively affecting, by means of collateral damage, the availability of services, business operations, market share, the confidence, as well as the reputation of the organization under attack. In this thesis, we leverage darknet data to investigate DDoS and DRDoS activities, which are special types of DoS events. In particular, we detect, analyze, predict and assess the threat behind their activities to generate DoS insights, which can be leveraged for situational awareness and mitigation purposes.

1.1 Objectives

The aim of this thesis is to generate cyber threat intelligence related to the inference of DoS activities. In this context, the thesis' objectives are listed below:

- Perform darknet data analysis and characterization.
- Provide inferences and insights related to DoS threats in addition to generate global cyber intelligence related to large-scale cyber activities.
- Investigate DoS activities in an attempt to predict their events and attribute such activities to certain campaigns as well as to certain Internet-scale malicious events.
- Develop approaches that can infer and assess the impact of large-scale DoS attacks and campaigns on the Internet.
- Design, implement and deploy a cyber security capability to infer Internet and DoS events.

1.2 Contributions

This thesis attempts to tackle the above-mentioned objectives. To this end, our contributions can be summarized as follows:

- Provide the first state-of-the-art survey on darknet research and the largest taxonomy of Internet passive monitoring.
- Leverage intrusion detection and data mining approaches on darknet for indicating cyber threat activities.
- Design and implement statistical and fuzzy hashing approaches for characterizing and inferring cyber campaigns of DoS attacks.

- Propose a prediction model based on time series techniques with capabilities to assess prediction, forecast and hence mitigate future DDoS threat occurrences.
- Propose a novel approach to fingerprint DRDoS activities through darknet analysis and identify the first real traces of large DNS reflection attacks.

In a nutshell, our work aims at studying darknet to generate DoS cyber intelligence. The latter could be adopted for immediate detection, mitigation and even attribution of DoS attacks.

1.3 Organization

The structure of this thesis is as follows. In Chapter 2, we primarily provide a background information on darknet. As a result, we define darknet and compare it to other trap-based monitoring systems. Furthermore, we provide some examples on its operation online. In Chapter 3, we provide a taxonomy in relation to darknet technologies and identify research gaps that are related to three main darknet categories: deployment, traffic analysis, and visualization. In Chapter 4, we elaborate on the work related to the investigation of darknet traffic, namely, characterization of its traffic and correlation among inferred threats. In Chapter 5, we describe the design and implementation of our DDoS prediction model. To this end, we also forecast DDoS cyber campaigns attempts. In Chapter 6, we elaborate on our novel approach to fingerprint DDoS reflection activities. Finally, Chapter 7 concludes this thesis, summarizes its contributions and highlights some research gaps that pave the way for future work.

Chapter 2

Background

This chapter provides an overview of darknet and highlights the focus of our survey by: 1) Providing definitions that list the alternative names; 2) discussing the differences between darknet and other trap-based monitoring systems; and 3) providing some examples of darknet and its operation on the Internet.

2.1 Darknet Definitions

The term darknet can refer to the following:

- Any communication system that operates by stealth and conceals its users' identity. Freenet [19] and BitTorrent [20] software are two examples that fit in this category.

- Servers and programs used to illegally distribute copyrighted material [21]. Such systems can include peer-to-peer file sharing technologies such as Napster and Gnutella [22].

- Servers configured to trap adversaries and collect suspicious data. This type of darknet runs in a passive mode without interacting with attackers. This is similar to the darknet project of Team Cymru [23].

In this work, we refer to darknet as per the last definition. Since these servers run in passive mode and correspond to unused hosts or devices, any observed traffic destined to them raises suspicion and hence necessitates investigation.

It is noteworthy to mention that the word darknet has been known under various alternative terms, including darkspace, blackhole monitors, unused IP addresses, network telescopes, unsolicited network traffic, unwanted traffic, non-productive or non-responsive traffic, spurious traffic, Internet background radiation (IBR), unallocated but reachable IP addresses and unassigned IP addresses. To harmonize the terminology, we use the word darknet throughout this thesis.

2.2 Trap-Based Monitoring Systems

Trap-based monitoring systems aim to deploy online sensors to trick and trap adversaries to collect malicious activities. Several systems leverage this approach such as darknet [8] and greynet [24]. A thin line separates various forms of trap-based network monitoring systems. In this subsection, several monitoring systems are contrasted and classified based on their types, interactivity levels, complexity, data collection and security aspects.

- *Darknet*: An IP address block configured in passive mode. Most of the darknet sensors return "unreachable" errors when a request is sent to listening hosts. This error explains that a certain host or port is not reachable. Darknet implementation is considered simple since these sensors do not communicate with the initiator of the communication. The captured traffic therefore consists mostly of the first request in communication.

- *IP Gray Space*: These addresses refer to devices that are not assigned to any host throughout a given time period (i.e., 1 hour, 1 day). Conceptually, IP gray space is similar to darknet; the only difference is that IP gray space addresses are unused only for a limited time, whereas darknet addresses are permanently unused. Unlike darknet, IP gray space might prove more difficult to be detected by an attacker since the underlying hosts might be active and operating as a regular machine during various periods of time. The aim is to imitate regular hosts.

- *Honeypot*: This is an interactive computer system, mostly connected to the Internet, that is configured to trap attackers. Honeypots are similar in nature to darknet but with more specific goals. Honeypots require more resources than darknet, since they interact during communication. As far as interaction is concerned, there are three major types of honeypots, namely, low, medium and highly interactive. A low-interactive honeypot is configured to interact with the initiator of the communication by emulating basic services such as replying to Internet Control Message Protocol (ICMP) ECHO request (i.e., Ping). A medium-interactive honeypot is similar to a low-interactive one but with further interactions and a greater number of emulated services for more data capturing and analysis. A highly interactive honeypot is a computer system that does not emulate services; it instead runs a fully-fledged, potentially vulnerable, operating system, services and applications.

- *Honeynet*: This network is simply a group of honeypots used to deploy distributed trap-based network monitoring systems for large-scale data collection and analysis.

- *Greynet*: This network is populated with active IP addresses interspersed with darknet addresses. In other words, greynet uses both darknet (passive) and honeypots (active) in the same monitoring IP address space. The purpose is to make the monitored IP space appear as a more attractive trap for adversaries. Take for example, a range of IPs that have both darknet and other active sensors running fake services. This scenario imitates a typical organization network that hosts both running and unused IP addresses, which may trick the attacker into thinking that the whole range of IPs in the monitored block is an appropriate target.

Table 2.1 provides a comparison of trap-based network monitoring systems based on several features: type of sensor, interactivity with the initiator, deployment complexity, data collection, and security of the monitoring IP address space. First, as mentioned earlier, darknet and IP gray space share similar features. These two trap-based monitoring systems are considered secure since they do not interact with the adversary. Furthermore, since they run in passive mode (null interactivity), their deployment difficulty and data gathering features are considered low compared to other monitoring systems. Second, regarding honeypots, the interactivity, the complexity and the data gathering features are mostly proportional to each other. For instance, the more interaction there is with the adversary, the more complex the implementation to setup and the greater is the amount of data that needs to be collected. However, all honeypots with an interactive feature are potentially vulnerable in terms of security. Finally, since greynet consists of darknet and honeypots, it is considered a more comprehensive monitoring system and could therefore have more possibilities in terms of interactivity, complexity, data collection and security.

Monitoring System	IP Type	Interactivity	Complexity	Data Collection	Security
Darknet	passive	null	low	low	secure
IP Gray Space	temporarily passive	null	low	low	secure
Low-Interactive Honeypot	active	low	low	low	vulnerable
Medium-Interactive Honeypot	active	medium	medium	medium	vulnerable
High-Interactive Honeypot	active	high	high	high	vulnerable
Greynet	active passive	low medium high	low medium high	low medium high	secure vulnerable

Table 2.1: Trap-based Monitoring Systems - Comparison

Figure 2.1 provides a graphical comparison between these major trap-based monitoring systems.

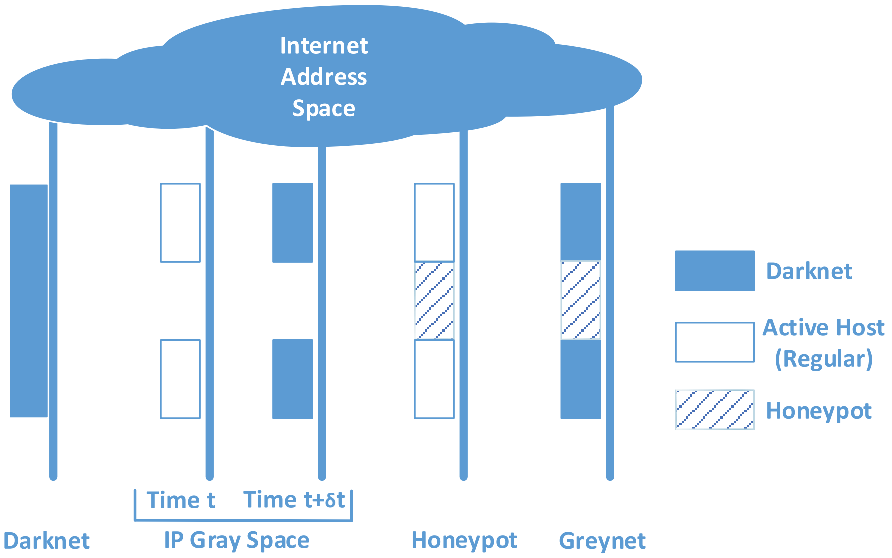

Figure 2.1: Trap-based Monitoring Systems - Address Space Distribution

First, the darknet contains only unused addresses running in passive (inactive) mode. Second, the IP gray space (at time $t + \delta t$) is similar to darknet. However, the same address space was already active in a previous period of time (time t). Third, honeypots can run in various modes, either solely on a network or with other active/passive hosts. The latter case represents the greynet address distribution.

It is worthy to mention that some monitoring systems have the capability to run in both darknet and honeypot modes, a feature, which allows honeypots to capture more data. Given that our aim is to investigate passive monitoring of unused IP addresses, the scope of our work covers mainly the study of darknet, greynet, IP gray space and few honeypots that solely target unused address space, such as Honeyd [25] and LaBrea Tarpit [26].

2.3 Darknet Inferred Cyber Threats

Darknet is indeed an effective approach to infer various Internet activities and threats related but not limited to the following:

Scanning/Probing or Reconnaissance Activities

Internet scanning is the task of probing enterprise networks or Internet wide services, searching for vulnerabilities or ways to infiltrate IT assets. Scanning can be initiated by computer worms, bots and other automated exploit tools. Scanning is a significant cyber security concern. The latter is due to the fact that probing is commonly the primary stage of an intrusion attempt that enables an attacker to remotely locate, target, and subsequently exploit vulnerable systems. It is basically a core technique and a facilitating factor for cyber attacks.

Distributed Denial of Service (DDoS) Attacks

DDoS attack is an attempt to make a computer and/or network resources unavailable. It consists of attacks that are deployed by one person or a group of people to temporarily or indefinitely shutdown services. The timing of such attacks can be coordinated to exploit the availability of critical organization infrastructure by directing enormous flood of Internet traffic to a small set of targeted IP addresses belonging to a target organization. By flooding the available bandwidth with intensive traffic, DDoS perpetrators can effectively bring down a service with potential loss of financial revenue. In addition, DDoS attacks can be coordinated via a botnet, which is a platform to orchestrate and manage cyber attacks.

Distributed Reflection Denial of Service (DRDoS) Attacks

DRDoS is a special type of DDoS attacks. In a typical DRDoS scenario, the attackers aim to hide their identities by leveraging third parties such as web servers and routers to redirect malicious traffic to the victim. In this case, all these third parties are called reflectors. Any host that responds to any incoming request can become a potential reflector. DRDoS threats have the ability to amplify attack traffic, which makes the threat even more severe. A well known type of DRDoS attacks is the

DNS amplification threat. In this attack, an adversary tries to generate a flood of tiny DNS requests, but with high amplified replies, on the Internet to reach open amplifiers. As a result, all amplified replies are sent back from these amplifiers (reflectors) to the victim.

More details on darknet activities and threats can be found in Chapter 3.

2.4 Darknet Operation

In this section, to achieve a better understanding on how darknet operates, we provide a brief background information related to some darknet scenarios. In particular, we show how darknet can be exploited on the Internet to generate various elements of cyber threat intelligence, including probing, DDoS and DRDoS activities.

A darknet is indeed an effective approach to infer various Internet-scale probing activities [27]. Figure 2.2 presents an illustrative example, in which a probing machine is scanning the Internet. Such machine could have been previously infected by a worm that is trying to propagate, or perhaps is participating in automated Internet-scale scanning [28]. Some of these network probing packets can hit the network telescope and thus are subsequently captured. Recall that the probing machine, while spraying its probes across the Internet, cannot probably avoid the network telescope as it does not have any knowledge about its existence. Further, it has been shown in [29] that it is extremely rare if not impossible for a probing source to have any capability dedicated to such avoidance.

Darknet traffic analysis is an effective technique in pinpointing victims of DDoS attacks [30]. Figure 2.3 illustrates such scenario. The attacker is directed to launch a DDoS attack towards the victim. To hide its identity, the attacker spoofs its address and replaces it with a random IP address. Such random address could happen to be that of the darknet. When the attack is launched, the reply packets from the

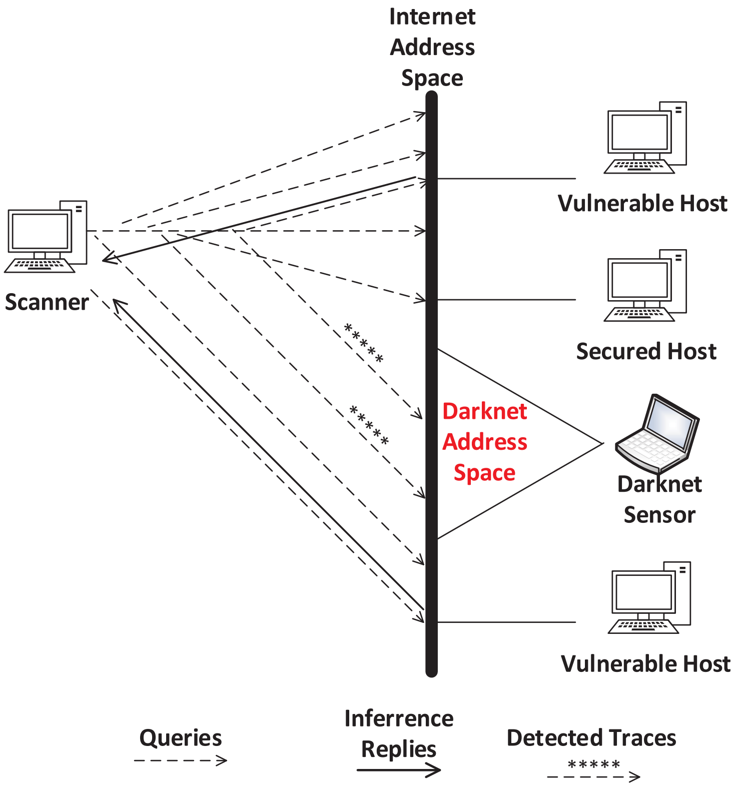

Figure 2.2: Probing Activities

victim will be directed towards some dark IP address. Traces that hit the darknet are often dubbed as backscattered packets [30] and could be effectively employed to infer that the victim has been the target of a DDoS attack.

In the last scenario, a darknet is leveraged to infer DRDoS attacks [31]. Indeed, as previously mentioned, such attacks are an emerging form of DDoS attacks that rely on the use of publicly accessible UDP servers [32][1], which act as "open amplifiers" of the attack. The bandwidth amplification factors are function of the instrumented protocol. The idea is to send small queries to such amplifiers in which the replies, that aim at flooding the victim, are orders of magnitude larger. Recall that such approaches are behind the notorious 300 and 400 Gbps attacks that hit the Internet in the last couple years [32]. More on amplification attacks can be found in Section 2.5.2. Figure 2.4 depicts this scenario. Commonly, the attacker will spray

[1] Although TCP amplifiers could be vulnerable to such abuse [33]

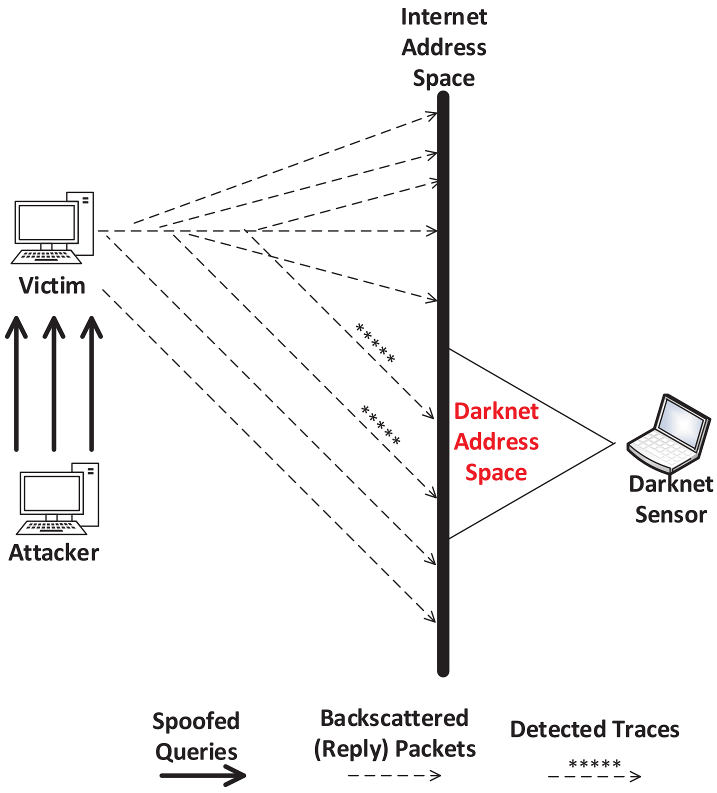

Figure 2.3: DDoS Activities

the Internet with such spoofed queries in a hope to reach as many open amplifiers as possible in order to achieve a large amplification factor. This case will occur in the scenario where attackers do not know in advance the IP addresses of Internet open amplifiers. We argue that such generated requests are not probes intended to gather information, since the attackers in this case do not aim to build/manage a list of open amplifiers nor do they want to jeopardize being detected (by using their real IP addresses, which is typical in probing activities). Intuitively, some of those requests will hit the darknet and hence will be captured. Requests that actually reach those servers will be amplified and directed towards the victim.

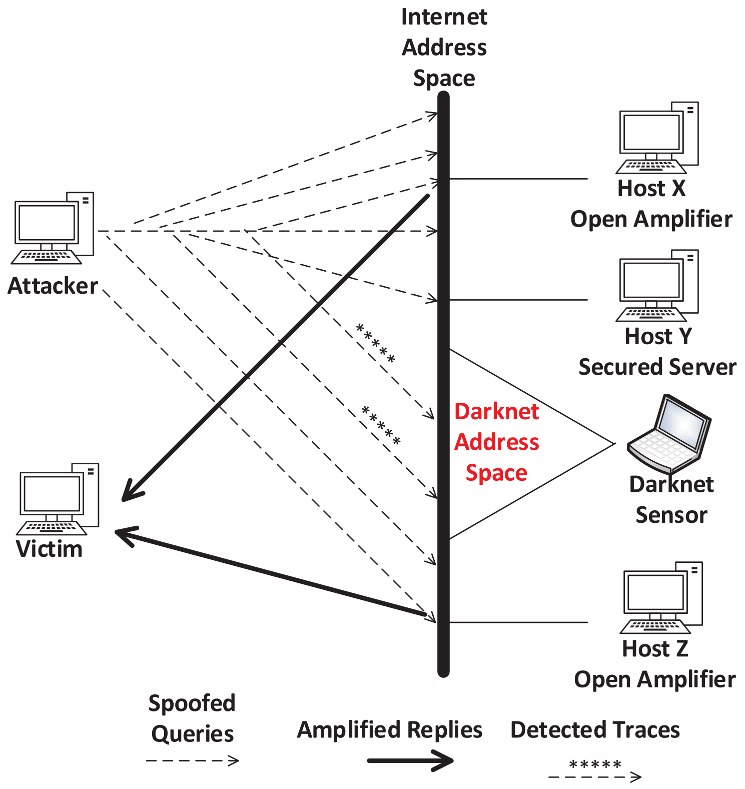

Figure 2.4: DRDoS Activities

2.5 DoS Attack Techniques

DoS attacks can be initiated in two major ways. The first is designed to consume host's resources. In this scenario, the victim could be a web service or proxy connected online. Obviously, any host has limited resources to process information. In a normal network operation, if the network flows exceeds this limit, the destination host starts dropping packets and informs the sender. As a result, legitimate senders slow down their sending rates to keep the operation balanced between the other host(s). In contrary, malicious users keep flooding victims to exhaust their resources, such as memory and CPU usage. The second way has impact on the consumption of network bandwidth, which could be more devastating than the first way. In this scenario, the attacks congest victims' network with corrupted or even legitimate flood of packets. Therefore, all benign requests of services destined to such victims will be partially or fully denied. To help readers gain a better understanding of such DDoS attacks, we list some well-known attacks in the following sections.

2.5.1 Protocol-based Flooding Attacks

Protocol-based attacks leverage vulnerabilities in Internet protocols to flood the victims with legitimate or corrupted packets. Some of the classical examples of these attacks are similar to SYN flooding and ICMP flooding. We describe the major flooding attacks below.

Transmission Control Protocol (TCP) SYN Flood

A SYN flood DoS attack exploits a known weakness in the TCP connection sequence, the three-way handshake, wherein a SYN request to initiate a TCP connection with a host must be answered by a SYN-ACK response from that host, and then confirmed by an ACK response from the requester. In a SYN flood scenario, the requester sends multiple SYN requests, but either does not respond to the host's SYN-ACK response, or sends the SYN requests from a spoofed IP address. Either way, the host system continues to wait for acknowledgment for each of the requests, binding resources until no new connections can be made, and ultimately resulting in a DoS attack.

User Datagram Protocol (UDP) Flood

This DoS attack leverages UDP, a session-less networking protocol. This type of attack floods random ports on a remote host with large number of UDP packets, causing the host to frequently check for the application listening on that port, and reply with an ICMP Destination Unreachable packet if the application is not found. This process exhausts hosts CPU and memory resources, and can ultimately lead to inaccessibility.

Internet Control Message Protocol (ICMP) Flood

Similarly, an ICMP flooding attack overwhelms the target resource with ping or ICMP Echo Request traffic. Such attack can exhaust both incoming and outgoing bandwidth capacity and can cause a delay or shutdown in services. A well known type of ICMP flooding threat is the Ping of Death (POD) attack.

Domain Name System (DNS) Flood

In a DNS flood scenario, malicious users target one or more DNS servers, attempting to bombard and turning down DNS root operations. In a typical DNS attack, the attacker attempts to overwhelming server resources and impeding the servers ability to direct legitimate DNS requests. DNS flooding are different than DNS amplification attacks. In general, DNS runs on top of UDP transport, which is a connection-less service. As such, spoofing DNS flooding attacks is more easily accomplished.

Hypertext Transfer Protocol (HTTP) Flood

HTTP is a well-known application layer protocol running on top of TCP port 80. HTTP flooding attacks hits web servers with a large amount of HTTP requests. HTTP requests can be crafted by attacks to avoid detection. These attacks are known to leverage botnet infrastructure to orchestrate attacks on one or many victims. The large usability of the web (`www`) services over the Internet has made HTTP flooding attacks popular and hence difficult to filter and detect.

Session Initiation Protocol (SIP) Flood

The recent deployment of Voice over IP (VoIP) telephony and its usability have created the SIP services. Unfortunately, attackers can leverage this technology to flood telephony services with DoS attacks. SIP services run generally on top of UDP port 5060. This telephony service is designed to provide easy service and use for legitimate services. Adversaries leverage vulnerabilities in SIP services, for example, to flood the victim with spoofed SIP invite packets.

2.5.2 Protocol-based Reflection Attacks

Recent events have demonstrated that amplification or reflection DoS attacks are probably the most effective and devastating cyber attacks. We list below the major ones such as DNS-based, NTP-based reflection attacks, among others.

Network Time Protocol (NTP) Amplification

NTP servers support `monlist` requests, which most NTP server implementations accept in their short form of only 8 bytes. Upon receiving a `monlist` request, an NTP server shares its recent clients in up to 100 UDP datagrams with 440 bytes payload each. One response datagram specifies statistics for NTP clients (such as the client's IP address, its NTP version and the number of requests) who contacted this NTP server. This response datagram is a useful debugging feature in the legitimate use case. The total response length depends on the number of client statistics a server shares upon request. An attacker can abuse this feature to amplify DoS traffic to a victim.

Domain Name System (DNS) Amplification

Name lookup (i.e., A or MX records), the traditional use case of DNS, have low amplification rates. Traditionally, the size of UDP replies was limited to 512 bytes and DNS switched to TCP communication for larger replies. However, many DNS servers adopted the DNS extensions (EDNS0) that allow for UDP responses of up to 4096 bytes. Attackers may abuse `ANY` request with EDNS0, for which a server returns all known DNS record types for a given domain. A well-known attack abuses

DNS open resolvers to function as amplifiers. Attackers can enforce high amplification rates by resolving ANY requests from domains that result in large responses. Attackers can even configure a domain they control such that its authoritative name server responds with 4096-byte-wide responses. Another reason behind this amplification is the deployment of DNSSEC, in which each resource record is accompanied with a typically 1024-bit-wide signature in a special RRSIG record.

Simple Network Management Protocol (SNMP) Amplification

Certain SNMP version (i.e., v2) supports the GetBulk operation, in which a device returns a list of SNMP identifiers that can be monitored. In the legitimate use case, this request can be used to iterate all monitoring values. An attacker can abuse this feature to amplify DoS traffic to a victim. The exact response size is determined by the number and length of identifiers in the returned item list.

Simple Service Discovery Protocol (SSDP) Amplification

Upon SSDP discovery requests, UPnP-enabled hosts respond with one reply packet per service they have configured. The response size depends on the configured services and the length of the service name. Some amplifiers respond with a few reply packets only, as they offer fewer services. An attacker could thus abuse this service by sending SSDP request packets spoofed with the victims IP address as the source of the request.

Character Generator Protocol (CharGen) Amplification

According to RFC 864, CharGen servers reply with random characters to incoming UDP datagrams of any length. An attacker may leverage this service on many servers and use small UDP packets with a spoofed victim IP address as the source to overwhelm the target.

Quote of the Day (QOTD) Amplification

Similar to CharGen, Quote of the Day servers (RFC 865) also send replies to UDP datagrams of any length. So an attacker may leverage this service on many servers and use small UDP packets with a spoofed victim IP address as the source to overwhelm the intended target.

Quake 3 Amplification

Quake 3 game servers are found to have the highest amplification when asking a server for its current status, a 15-byte-wide request. The reply is significantly larger and includes, i.e., the detailed server configuration and a list of current players. Given a number of Quake 3 servers with a large number of users currently active on the server; an attacker may leverage this service on any number of Quake 3 servers by sending status requests to the server and replacing the source IP address with that of the victim in order to overwhelm the target.

Network Basic Input/Output System (NetBios) Amplification

For NetBios, an attacker may achieve DoS amplification using a name lookup, for which a receiving Windows system responds with its current network and host name configuration. The response sizes are influenced by the host names and network configurations of the amplifiers. An attacker may send requests to a NetBios capable server spoofing the victims IP address as the source so that the victim receives the overwhelming reply traffic.

2.5.3 Summary

We have presented several DoS attacks, namely, flooding and amplification. It is noteworthy to mention that the types of threats are not always mutually exclusive.

In practice, an adversary might leverage several features of multiple types in only one attack. For instance, TCP SYN flooding and ICMP flooding are generally initiated simultaneously against DNS root servers. As far as our approach is concerned, based on the aforementioned inference techniques of Section 2.4, we are able to identify all the aforementioned types of attacks only if their traces hit our darknet sensors.

2.6 DoS Defense Mechanisms

In general, there are three defense mechanisms against DoS attacks, namely, attack prevention and mitigation, attack detection, and attack attribution. Attack prevention aims to fully/partially block the attack or successfully handle its flood. Attack detection identifies the occurrence of the attack. Finally, attack attribution identifies the source of the attack. It is noteworthy to mention that a complete DoS defense mechanism consists of prevention, detection and attribution techniques.

2.6.1 Attack Prevention and Mitigation

The aim of attack prevention and mitigation is to completely or partially block the attack before causing any interruption of service. As shown earlier, since DoS attacks are generally initiated from spoofed (fake) IP addresses, some of the best techniques used to block such threats are to leverage ingress/egress filtering [34]. The latter is an efficient technique to control incoming and outgoing packets on the local or Internet network. For instance, an organization can block all outgoing packets coming from (leaving) its network if they do not have source IP addresses registered under the name of this organization. The same technique can be implemented at any Internet service provider or Internet backbone associations. One of the protocols that operate based on the same concept is the Source Address Validity Enforcement (SAVE) [35]. Moreover, some techniques are protocol-dependent and are designed with security features to prevent or mitigate DDoS. For instance, the

Stream Control Transmission Protocol (SCTP) [36] runs on the transport layer with advanced security features to defend against TCP SYN flooding attack. Although this protocol can mitigate the threat of SYN flooding, its implementation requires more attention because it may cause other types of DDoS such as the ones using malformed ICMP packets and `INIT` (initialization packet) flooding attack [37]. Similarly, the Datagram Congestion Control Protocol (DCCP) [38] has a mechanism to allow the server to avoid holding any state of unacknowledged communication during a handshake. Since the development of DCCP is relatively new, developers must be very careful while implementing DCCP services. For instance, one of the DoS security concerns can happen when associating applications with service codes[2]. This operation requires additional processing time to interpret information and hence may cause a DoS attack. Last but not least, a recent implementation of cloud-based DDoS protection mechanisms [39] leverage several servers to act on behalf of the victim during an attack. The latter technique is more recent than the other ones and is found to be efficient, but not perfect, to mitigate the impact of attacks [40].

2.6.2 Attack Detection

The most effective way to defend against DoS attacks is attack prevention. However, since adversaries are always discovering new techniques to attack a victim, prevention may not be always successful. Therefore, attack detection is also a fundamental step to defend against DoS attacks. This technique can help in fingerprinting a malicious flood and provide useful insights on several attack parameters such as rate, attack type, signature, CPU and memory usage, among others. Attack detection techniques leverage several algorithms, namely, flow-based, signature-based and anomaly-based. Flow-based algorithms leverage the flood parameters (i.e., attack speed, nature of packets) to detect attacks. For instance, the approach proposed by

[2] Internet Engineering Task Force: The DCCP Service Codes

Moore et al. [30] is a typical flow-based detection algorithm that leverages backscatter packets to infer DDoS activities. Signature-based algorithms leverage packet information to match a malicious activity based on a database of signatures. This method cannot identify zero-day (new) DoS attacks. A network-based intrusion detection system such as snort [41] runs such algorithms. While signature-based algorithms can identify solely known attacks, anomaly-based approaches use training models and pattern recognition techniques to identify floods of old/new DoS threats.

2.6.3 Attack Attribution

Attack attribution aims at identifying the source of attack and affiliating them with a specific IP address. Since DoS attacks are usually leveraging spoofed IP addresses, the attribution of attacks is a difficult problem. In fact, IP spoofing is still a fundamental weakness of Internet operations. Two reasons are behind this issue. First, the availability of tools and techniques to initiate packets with forged IP addresses. Second, the stateless nature of Internet routers, which generally store information and forward packets to the next hop only. Some of the attack traceback techniques that are used include active interaction, probabilistic and hash-based schemes. First, a main feature of the active interactive approach is that on the way to the victim, routers interact with adversaries in a certain way (i.e., forwarding requests). As such, this technique traces the source of the attack based on the reaction of flood during the attack. Second, in general, probabilistic IP traceback models leverage the fact that routers probabilistically insert fragmentary network path data in the incoming packets. As such, this technique attempts to reconstruct the flow path using these inserted information. Finally, many probabilistic approaches can fail, especially when large-scale DoS attack traffic is distributed over many routers in different locations. Consequently, a hash-based IP traceback approach is proposed to store information on each packet passing through routers. Regardless of the technique used in addressing DoS attribution and spoofing, this problem is still a major concern for Internet users.

2.6.4 Summary

We listed above the major defense mechanisms against DoS attacks. We divided the techniques over three categories, namely, attack prevention and mitigation, attack detection, and attack attribution. Although darknet can be used to attribute DDoS attacks [42], our approach falls mainly in the attack detection research area. Obviously, uncovering the type of the attack, and the techniques behind it can help in understanding the malicious behavior and hence can solve the problem. Therefore, our analytics and assessment of attacks can be leveraged by academia and industry to help in preventing, mitigating, and attributing DoS cyber attacks.

Chapter 3

Darknet Taxonomy

Despite the fact that the idea of monitoring unused IP addresses started in the early 90's [9, 43], we provide a background information that mainly focuses on the study of darknet research during the past thirteen years. The reason behind choosing this period is that the major contributions started after 2001.

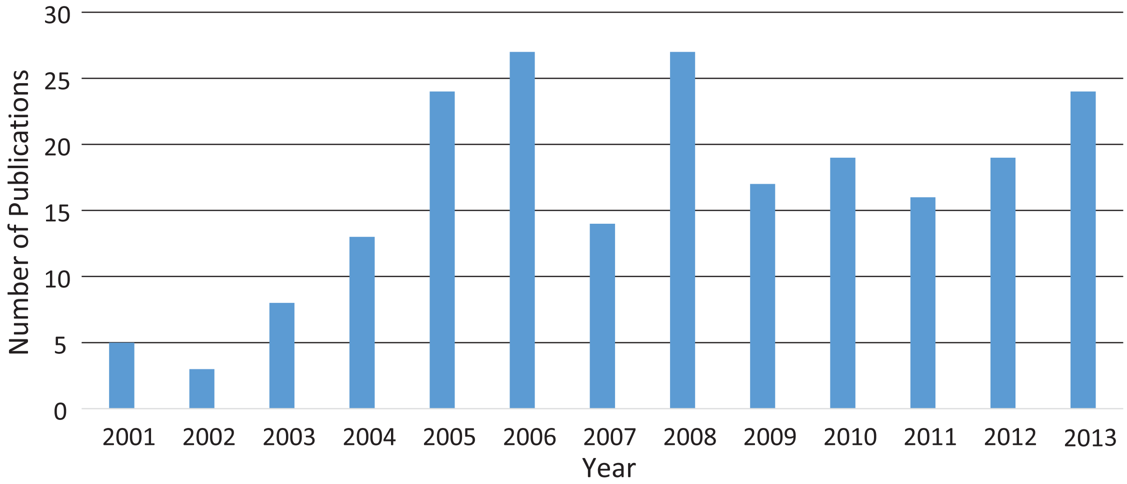

Figure 3.1: Trend of Publications Per Year

Figure 3.1 represents the trend of the darknet research from 2001 to 2013 in terms of research publications. Some of the important contributions include the discovery of the relationship between backscatter traffic and DDoS attacks, which emerged in 2001 [30], the trend of worms propagation and analysis between 2003 and

2005 [44–46], the use of time series and data mining techniques on darknet traffic raised in 2008 [47], and finally the monitoring of large-scale cyber events [11], which began in the past few years.

Our taxonomy classifies current darknet research into three major areas, namely, darknet deployment and setup, analysis and measurement of darknet data through deployed sensors, and tools and techniques for the visualization and representation of its traffic. A high level overview of the proposed taxonomy is shown in Figure 3.2.

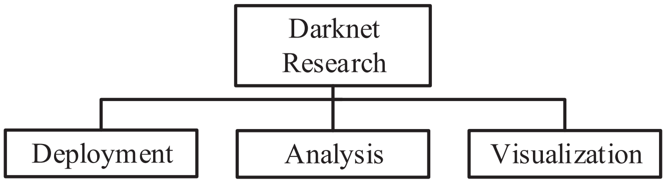

Figure 3.2: Darknet Research Taxonomy

3.1 Darknet Deployment

The first step in darknet monitoring is the deployment of sensors, which aims to capture network traffic. This exercise requires an understanding of the network architecture and a careful configuration of the dynamic host server or the upstream router to forward unreachable packets to darknet sensors. A basic darknet deployment architecture is shown in Figure 3.3.

This section provides insights on the elements of darknet deployment, namely, darknet variants, as well as techniques such as sensor placement/identification and data handling, and projects. Figure 3.4 provides a taxonomy of deployment research works based on the aforementioned elements.

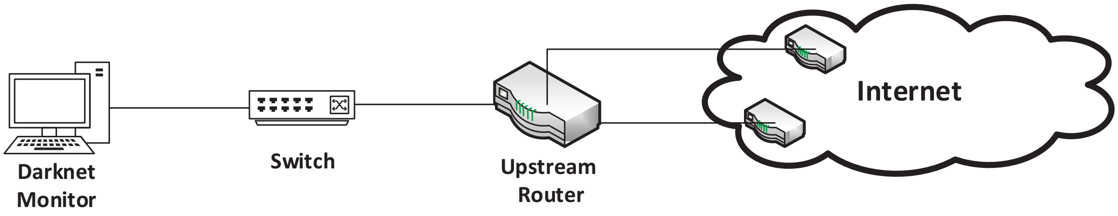

Figure 3.3: Basic Darknet Deployment - Inspired by [1]

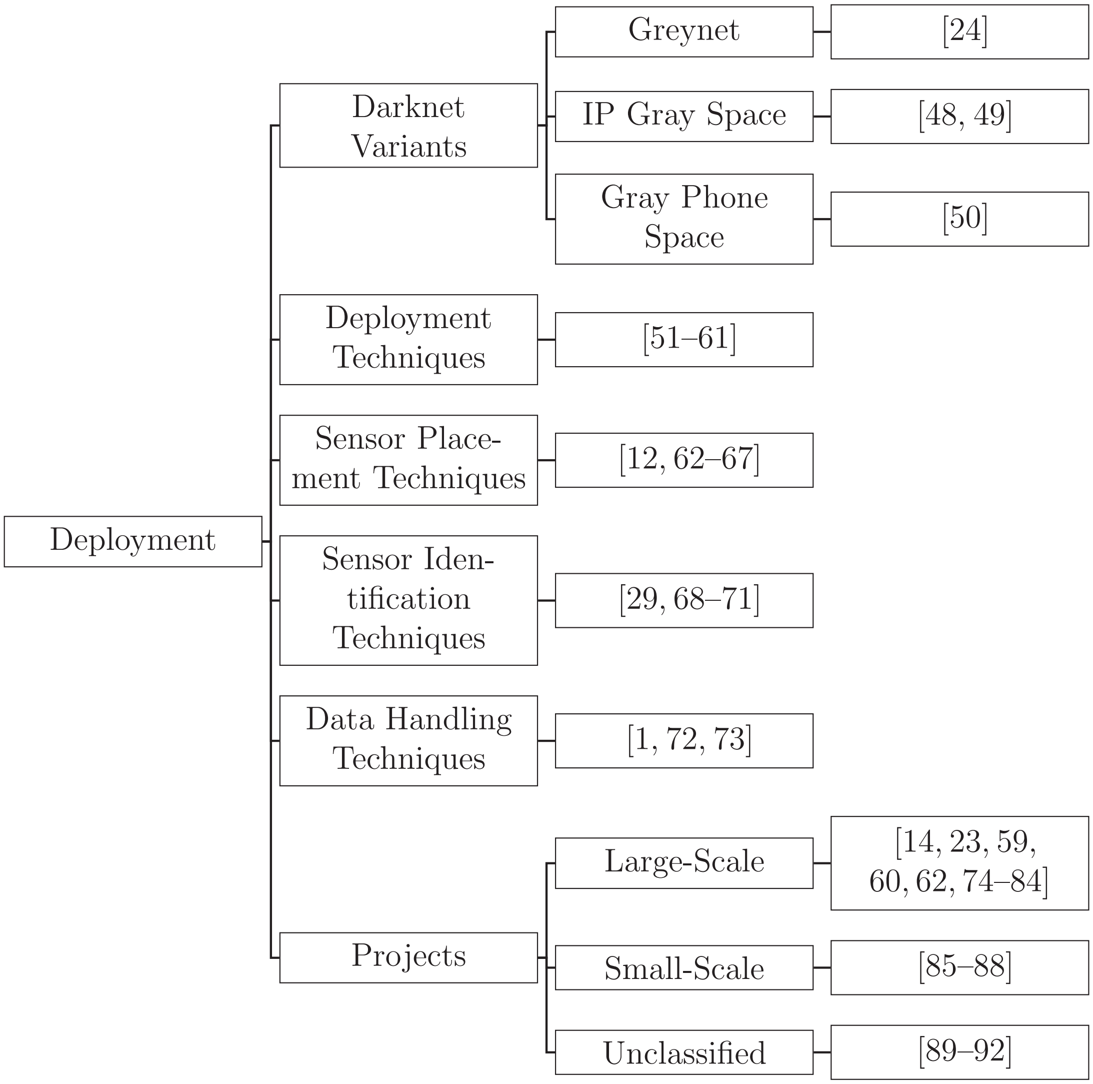

Figure 3.4: Deployment Research Taxonomy - Overview

3.1.1 Darknet Variants

Recalling Section 2.2, darknet variants are the deployment mechanisms of trap-based monitoring systems using techniques similar to those of a darknet. This part thus includes deployment of IP gray address space and greynet monitors. Table 3.1 summarizes the papers on darknet variants.

Publications	Approach/Technique	Contribution	Tool/Project
[24]	Defining and Characterizing	Greynet Development	Custom
[48]	Heuristic Algorithm	IP Gray Space Development	Custom
[49]	Heuristic Algorithm	IP Gray Space Development	Custom
[50]	Statistics	Gray Phone Space Development	Greystar

Table 3.1: Darknet Variants Research Papers - Summary

Harrop et al. [24] define and assess the concept of a greynet, a network address space that is populated with darknet addresses mixed with active IP addresses. Using data collected from a university network, the authors evaluate their concept and show how a small number of dark IP addresses can increase the efficiency of network scanning detection. Furthermore, Jin et al. [48, 49] are among the pioneers to use IP gray space in passive monitoring. This work applies a heuristic algorithm to identify IP gray space addresses. The authors investigate the behavior of such traffic. This study tackles patterns such as dominant and random behaviors. The approach identifies the usefulness of IP gray space to uncover insights on the behavior of malicious activities as well as their intentions. The result identified several malicious activities such as scanning, worm propagation as well as spam. Finally, in a unique work, Jiang et al. [50] investigate passive monitoring in mobile communication. This work presents a novel approach to detect SMS spammers on a cellular network. The approach is based on greystar technology and employs a statistical model to infer spam size through fingerprinting. The proposed approach also has the capability to reduce the spam traffic by 75% during peak periods. The authors analyzed five months of SMS data from large cellular networks and inferred thousands of unreported spam activities.

3.1.2 Deployment Techniques

In this section, we discuss the research works that mainly target the techniques of deploying passive monitoring systems. Table 3.2 summarizes these contributions. In this category, research works are mainly leveraging Intrusion Detection Systems (IDS) and hybrid techniques.

Publications	**Approach/Technique**	**Tool/Project**
[51]	IDS	honeyd/DShield/DOMINO
[52]	Sink - IDS	iSink
[53]	Sink - IDS	honeyd/iSink
[54]	Statistics - IDS	Custom
[55]	Mobile-Based AS Data	honeyd/Mohonk
[56]	Hybrid	honeyd
[1]	Hybrid	IMS
[61]	Hybrid	Custom
[58]	Comparative Study	honeyd
[57]	Hybrid	IMS

Table 3.2: Deployment Techniques Research Papers - Summary

Yegneswaran et al. [51] introduce a scalable, heterogeneous, and robust Distributed Overlay for Monitoring InterNet Outbreaks (DOMINO). The proposed approach provides an architecture for collaboration of distributed IDS data on different nodes on an overlay network. In an overlay design, a network is built on top of another one. One of DOMINO's components is the use of active nodes, which measure connections targeting unused IP addresses. The authors emphasize the importance of the approach in detecting sources of IP spoofing, classifying cyber attacks, generating updated blacklists and reducing false positives. Moreover, Yegneswaran et al. [52] introduce iSink and elaborate on a darknet case study to analyze attack traces. The study is composed of various components such as the analysis of backscatter packets and the investigation of unique periodic probes. iSink deployment proved its relevancy in detecting worms such as Sasser. Through iSink, the authors managed to observe different worm variants and malware. Furthermore, Yegneswaran et al. [53] explore ways to integrate trap-based monitoring information, including darknet data, into daily network security monitoring with the goal of sufficiently classifying and summarizing the data to provide ongoing situational awareness. To this end, the authors develop a system based on honeynets, analyzers that leverage Network-based Intrusion Detection System (NIDS), and a back-end database to facilitate the analysis of honeynet data. The system is able to capture and identify numerous malicious activities including botnet and worms.

Choi et al. [54] propose a framework to monitor and respond to security events. The approach aims to trace potential attackers using darknet. The approach was evaluated using a `/24` darknet IP address block and other alert logs. Several attack trends and patterns were identified. In addition, the approach showed capabilities to detect zero-day attacks. Furthermore, Krishnamurthy et al. [55] propose a mobile darknet-based mechanism that allows unwanted traffic to be detected significantly closer to the origin source of attack. The scheme is based on two pieces of information: the additional data that is made accessible to the upstream autonomous systems (AS) and the changes in the advertised darknet. Such shared data among ASes can identify and minimize unwanted traffic between these entities.

Bailey et al. [56] propose a hybrid monitoring architecture that uses low-interaction honeypots (honeyd) as front-end filters and high-interaction honeypots as a back-end for further investigation. In order to reduce loads on back-ends, a filtering mechanism is used coupled with a novel hand-off mechanism. The authors use five months of data to demonstrate the efficiency, scalability and robustness of their work. In addition, Bailey et al. [1] discuss the major elements of darknet deployment setup, namely, the storage and network requirements and the deployment techniques. They further review the methods to collect darknet data and list the most suitable formats. They propose three major darknet deployment approaches to build darknet sensors. Moreover, Bailey et al. [57] examine the singular and distributed passive monitoring sensors to effectively build a scalable hybrid monitoring system. The authors demonstrated that the majority of the threats coming to darknet were based on a limited number of source hosts, and proposed a new source-distribution approach to reduce the number of events found while investigating darknet data. The analysis listed several threats including worms and scanning activities.

Pouget et al. [58] provide a thorough comparison between honeypots based on their level of interaction. Using honeyd as a low-interactive honeypot, this qualitative and quantitative comparison uncover interesting classification and correlation among detected threats. Finally, Komisarczuk et al. [61] discuss the opportunities and research directions in the Internet sensor grid for detecting and analyzing malicious behaviors online. The authors review the developments of monitoring sensors in active and passive modes. They further share their experiences in sensor deployments.

3.1.3 Sensor Placement Techniques

This category includes techniques that are used to improve sensor placement and setup. Table 3.3 lists the relevant research works.

Publications	**Approach/Technique**	**Tool/Project**
[62]	Hybrid	IMS
[63]	Comparative Study	honeyd/Leurre.com
[66]	Multiscale Density Estimation	iSink/DShield
[65]	Comparative Study	DShield
[64]	Empirical Analysis	Netflow
[67]	Sampling	Custom
[12]	Comparative Study	IMS

Table 3.3: Sensor Placement Research Papers - Summary

Several techniques have been used to improve darknet monitors placements. For example, Cooke et al. [12] examine variations observed on different network blocks. The authors showed evidence that distributed address blocks exhibit significant changes in traffic patterns. They further demonstrated changes over protocols (services) and specific worm signatures. Moreover, Bailey et al. [62] examine the properties of individual and distributed darknet sensors to test the effectiveness of deploying hybrid systems (darknet with honeypots). The authors used source-based techniques to reduce redundant actions generated by individual darknet and hence lowered the evaluated connections by over 90%. They also expanded source-distribution based techniques to detect a variety of global attacks. Furthermore, Chen et al. [63] demonstrate the importance of deploying multiple sensors in different locations. The authors deployed two identical sensors, having the same configurations, in two different locations and compared various parameters. While analyzing data from a six-month period, the analysis revealed different anomalies. Likewise, Berthier et al. [64] focus on the size and the location of darknet sensors to perform an empirical analysis and increase the efficiency of darknet monitors. In addition, Abu Rajab et al. [65] quantify the importance behind the design of a distributed monitoring system and evaluate the applicability of this approach. In order to achieve their goals, the authors propose a worm propagation model to evaluate the locations of monitors, the size of the monitored IP addresses, and the impact of worm detection time. Over 1.5 billion suspicious connection attempts were observed through many detection systems across the Internet. The results showed that distributed monitoring systems were better than centralized ones. In terms of speed, a distributed monitor system was found to act four times faster than a centralized one. Furthermore, the authors mentioned that monitor placement can be improved by having partial knowledge of the vulnerable population density. In some cases, exploiting information related to vulnerable host locations can help decrease the detection time by seven times compared to random monitoring deployment. Furthermore, Barford et al. [66] present a study of source locations of hosts that send unwanted traffic through dark addresses. The researchers use a multi-scale density estimation method which allowed them to see a small number of tight clusters that are formed by darknet source addresses. The authors propose a multiplicative model for darknet host locations that can be used to generate data with the same distributed property as empirical data. Their model can be used for testing, evaluating, measuring, simulating and analyzing traffic for the purpose of reducing darknet pollution. Finally, Pemberton et al. [67] outline results from a `/16` darknet network by experimenting with various sampling techniques and applying them to arrival density measures. The authors found that current darknet deployments using continuous lists of IP addresses were inefficient in predicting threats. They further studied three other address space allocation techniques and discovered better accuracy. The researchers claim that business users as well as Internet Service Providers (ISPs) can use these techniques to enhance darknet deployment in the future.

Publications	**Approach/Technique**	**Contribution**	**Tool/Project**
[70]	Marking Algorithm	Detecting Listening Sensors Online	Custom
[71]	Probe Response Attack	Proposing a Technique to Detect Sensors	Custom
[69]	Automatic Profiling - Random Sampling	Discussing Sensor Identification and Configuration	Custom
[29]	Perspective-Aware Address Discovery	Proposing a Model to Uncover Darknet	Dark Oracle
[68]	Sampling	Highlighting an Evasive Attack that Identifies Sensors	DShield

Table 3.4: Sensor Identification Research Papers - Summary

3.1.4 Sensor Identification Techniques

This part includes research targeting the identification of darknet sensors. From the adversary's point of view, the identification of monitoring sensor locations allows them to avoid detection. Table 3.4 summarizes these related works. Abu Rajab et al. [68] highlight an evasive attack that detects passive monitoring systems such as darknet. By sampling the IP address space in a coordinated manner, the authors show that detection and evasion of monitors is possible. Using this technique, attackers can identify active hosts on the network and hence proceed with their attacks. The proposed methodology can overtake the entire vulnerable population within seconds. In a similar work, Sinha et al. [69] elaborate that monitoring sensor configurations are easy for attackers to discover. The authors discuss that manually building a monitoring system is usually a large and difficult task to handle. Therefore, the authors propose an automated technique for sensor configuration. They further argue that networks with consistent nodes and proportional representation are more efficient in detecting attacks and more resistant to detection. Using random sampling and profiling, the authors propose a technique for automated configuration of sensors. More on identifying monitors' locations, Shinoda et al. [70] propose several algorithms that are designed to detect listening sensors on the Internet. Consequently, they propose an approach to enhance the sensor setup and deployment. In a similar work, Bethencourt et al. [71] demonstrate the use of probing to detect sensors' locations on systems that publicly report security results. This probe response technique, which can target darknet sensors, shows how to locate monitors. With limited capabilities, the simulation results of this technique illustrate the power of determining the sensors' identity within one week. The authors further target the anonymized schemes used by network administrators and discuss some potential countermeasures based on the sensors' characteristics. Finally, Cooke et al. [29] propose the Dark Oracle, which is an architecture that aims to uncover dark addresses. The authors validated the effectiveness of their work, which uses internal as well as external routing and host setup information for automatic discovery. The proposed methodology uncovered almost 80,000 unique source IPs compared to 4,000 with a traditional `/24` darknet. The authors further demonstrated the capability of the Dark Oracle by shedding light on local attacks.

3.1.5 Data Handling Techniques

Deploying darknet requires handling data, which includes processing, storing and sharing its traffic. Darknet may receive a large amount of unsolicited network traffic. Processing such information at the sensor level and sharing it with investigators and researchers may therefore require several development steps. Table 3.5 summarizes the data handling research papers.

Publications	**Approach/Technique**	**Tool/Project**
[72]	Resource-Aware Multi-Format Data Storage	IMS
[73]	Graphical Processor	Custom

Table 3.5: Data Handling Research Papers - Summary

In this category, Cooke et al. [72] propose a resource-aware multi-format data storage of security information with the aim to simultaneously save various security information. The proposed architecture consists of a set of algorithms for storing various formats of data. Furthermore, a darknet-based prototype is built based on numerous sources of data and the results show reasonable short- and long-term outputs. Moreover, Nottingham et al. [73] suggest graphical processors to accelerate darknet big data analysis. They further discuss the construction, the performance and the limitations of the packet filtering approach, which employs multi-match capabilities to differentiate between packets. The aim is to build a fully programmable virtual machine with massive parallel classification, data mining and data transformation capabilities to provide complex security filtering, indexing and manipulation functions.

3.1.6 Projects

The outcome of deploying darknet sensors is to build a functional platform, an operational project or center to monitor the cyberspace. We list below the publicly

Project	Stewardship	Description	Objectives
UCSD Network Telescope [76]	CAIDA	Passive traffic monitoring system built on a globally routed /8 network	Monitoring of DDoS, Internet worms, viruses, scanning and data sharing
ATLAS [14]	Arbor	The world's first and largest globally scoped threat analysis network	Providing global threat intelligence for DDoS and advanced threats
The Darknet Project [23]	Team Cymru	Internet security research and insight	Monitoring compromised machines from malware
IMS [84]	University of Michigan	A distributed global Internet threat monitoring system of /8 network	Measuring, characterizing, and tracking threats
PREDICT [93]	RTI	Protected repository for the defense of infrastructure against cyber threats	Investigating spatial and longitudinal darknet data
NICTER [78]	NICT	A large-scale network incident analysis system	Visualizing and analyzing network attacks
WOMBAT & Leurre.com [79]	EURECOM	Worldwide observatory of malicious behavior and attacks threat	Studying cyber attacks and threats
Internet Storm Center & DShield [83]	SANS	A global cooperative cyber threat, Internet security monitor, and alert system	Monitoring the level of malicious activity on the Internet

Table 3.6: Large-Scale Darknet Projects - Summary

known centers and projects that use darknet as a source of their data. Table 3.6 summarizes large-scale darknet monitoring projects. Our classification is based on three groups, namely, large-scale, small-scale and unclassified projects.

The first group in this area lists large-scale darknet projects. For instance, the network telescopes project [76, 94] is a system proposed by researchers at the Center for Applied Internet Data Analysis (CAIDA). The intent of this project is to monitor pandemic and epidemic cyber incidents through the unused address space. Moore et al. [75] propose the network telescope as an efficient and effective darknet traffic monitoring system by using sensors and virtual machines. The network telescope project can monitor large chunks of unused address space. The University of California, a main contributor to this data, deploys network telescopes to monitor a single unused Internet address space of /8 block. The latter represents around ${\frac{1}{256}}^{th}$ of the overall IPv4 address space of the Internet. Collected data includes Domain Name System (DNS) data, topology traces, round-trip time, and routing data. This passive information contains insights about large-scale security events such as malware (mostly Internet worms) and DDoS. Another project is the Active Threat Level Analysis System (ATLAS) [14], the Internet's first globally scoped threat analysis network. Under the direction of Arbor Networks, this network monitoring system collectively analyzes the data traversing disparate darknet to visualize malicious activities on the Internet. Arbor is among the unique operators positioned to provide enterprise and service provider-specific intelligence related to malicious activities such as exploits, phishing, malware and botnet. In addition, the Darknet Project [23] is deployed by the Team Cymru Community as a passive Internet threat monitoring system. Its main purpose is to set a platform to collect packets susceptible to be sent by malware. This darknet is deployed to host flow collectors, backscatter detectors, packet sniffers and IDSs. Team Cymru aims to increase awareness about threats and enhance mitigation against malware. In addition to monitoring darknet, the authors provide a guideline to set up a darknet. Another large-scale project is the Internet Motion Sensor (IMS) [62], a distributed globally scoped Internet threat monitoring system. The IMS project has the ability to monitor dark IP space. It uses 28 unused IP blocks, ranging in size from /25 to /8 network address blocks. The IMS is based on a distributed blackhole network with a lightweight responder, a payload signature and a caching mechanism. These capabilities are used to generate new insights about worms, DDoS, and scan activities [84]. Furthermore, the Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT) project [93] investigates spatial and longitudinal darknet data. The authors aim to describe some of the large-scale spatial and longitudinal darknet information. Another large-scale project is the Network Incident analysis Center for Tactical Emergency Response (NICTER) [77, 78], which is a large-scale network incident analysis system that mainly monitors darknet. It represents a system that is capable of capturing and analyzing malware executable. The identification of malware propagation is the primary purpose of this project. The NICTER project is composed of four components: macro analysis system, micro analysis system, network and malware enchaining system, and the incident handling system. Additionally, the Worldwide Observatory on Malicious Behavior and Attack Threats (WOMBAT) [59, 74] center aims at providing new artifacts to understand emerging threats. The project WOMBAT is used to collect raw data and analyze it in order to identify different threat phenomena. The authors claim that the latter can discover trends of attacks by understanding the behavior of threats. With this in mind, the designers develops mechanisms for automatically collecting and analyzing malware [95]. WOMBAT has a number of features. Its main feature is to improve data acquisition technologies. The project further shares information with its partners, including SGNET [96], *Leurre.com* [79], Argos [97], Nepenthes [98], NoAH project [87], and SANS Internet Storm Center (ISC) [83, 99] which uses the DShield as firewall [100]. Moreover, The *Leurre.com* Project [60, 80], a part of the WOMBAT project, has a purpose of collecting Internet threats using worldwide distributed sensors [79]. The terms used in the context of this project include platform architecture, logs collection, data uploading mechanism and data enrichment mechanism. Furthermore, the Billy Goat project [81] is a specialized darknet traffic monitoring system deployed by IBM and its customer networks. It is used for worm detection. This project differs from other monitoring systems as it focuses on specific attacks and dynamic characteristics of worms. By taking advantage of worm propagation strategies, Billy Goat monitors unused IP address spaces that are randomly scanned by worms. Finally, the Honeynet project [82] is a dedicated system to investigate cyber attacks and develop open source security techniques to mitigate Internet threats. This project provides tools to build darknet sensors.

The second group in this category are small-scale projects. For example, Antonatos et al. [88] propose HoneyHome, a part of the NoAH project [87], a platform for monitoring unused IP addresses and ports for large-scale security events extraction. This low-cost system is based on installing sensors on regular users to monitor these unused IP addresses and ports. Since regular users come and go, it is difficult for attackers to detect these unstable sensors. Moreover, ARAKIS [86], one of the initial data sources for WOMBAT, is developed by NASK and operated by CERT Polska. The latter project is a nationwide near real-time NIDS that generates early notifications and warnings about security events. The system consists of a central database in addition to distributed monitors, which collect and correlate security information through low-interaction honeypots and other detection systems including darknet. Finally, Daedalus [101], which is based on the NICTER project, is designed to capture cyber attacks in near real time fashion.

Last but not least, it is worthy to mention some other unclassified projects that use passive monitoring such as SWITCH [89], the National Police Agency of Japan [90], the Internet Scan Data Acquisition System (ISDAS) runs by Japan CERT Coordination Center [91], the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) [102], the IUCC/IDC Internet Telescope [92] in Israel, the Simwood Darknet [103] and many other academic systems such as the Darknet Mesh Project [104] at Oxford University as well as Rhodes University Network Telescope [105].

3.1.7 Summary

We have discussed several key elements in the darknet deployment section, namely, architecture, darknet variants, online placement and identification of sensors, data handling, and projects. From what has been discussed in the deployment part of Section 3.1, we can conclude the following points:

- In order to deploy darknet, several elements must be taken into consideration, such as the study of exact storage and network requirements, the knowledge of deployment techniques, as well as sensor placement and identification.

- Compared with other trap-based monitoring systems, darknet is considered as a practical and easy-to-implement tool in passive monitoring the cyber space. Darknet setup can be developed using basic routing techniques and monitored through IDSs.

- IDSs are the most used systems in darknet development and Honeyd is probably the most practical tool to implement darknet sensors.

- One of the major challenges in deploying darknet is to avoid the adversary's discovery of the sensor location. Several techniques are used to identify the location of sensors such as the sampling of IP addresses.

- Mobile darknet is a new trend that has a promising future in passive monitoring research. The future deployment will include mobile-based VoIP darknet.

- Darknet variants are not commonly used in literature. These variants can be more efficient than darknet to monitor cyber attacks; however, their implementation could be more complex.

- Darknet projects monitor various cyber threat activities and are distributed in one third of the global Internet.

- Various types of darknet projects exist. Some large-scale projects are coupled with interactive trap-based monitors to enhance network monitoring.

- CAIDA is one of the few Internet monitoring research groups, which provides darknet-based backscatter data for researchers.

- Despite the existence of some collaborative darknet projects (i.e., PREDICT), more darknet resources and information sharing must emerge to infer and attribute large-scale cyber activities. Dealing with a worldwide darknet information exchange is a capability that requires collaboration and trust; however, this collaboration raises security policies and privacy concerns.

In the next section, we provide a taxonomy of darknet data analysis.

3.2 Darknet Analysis

This section provides an overview of the contributions in the area of darknet data analysis and measurement. These topics are divided into three main areas: analyzing and measuring darknet data, threats, and worldwide events. Figure 3.5 depicts the taxonomy of research efforts in the analysis and measurement of passive monitoring systems.

3.2.1 Data Analysis

In this section, we provide a taxonomy of the research works related to darknet data. This includes profiling darknet traffic, filtering and classification of its data as well as reviewing its backscatter and misconfiguration traffic.

Data Profiling

Data Profiling encompasses the research works that focus on the characterization of darknet data to generate statistics and insights. Table 3.7 provides an overview of the summarized research works. These contributions leverage several techniques such as packet filtering, routing, and time series.

For instance, Irwin [106] explores data across five different darknet sensors. The author discusses the differences as well as the similarities among the analysis of the five sensors and presents two case studies related to two vulnerabilities

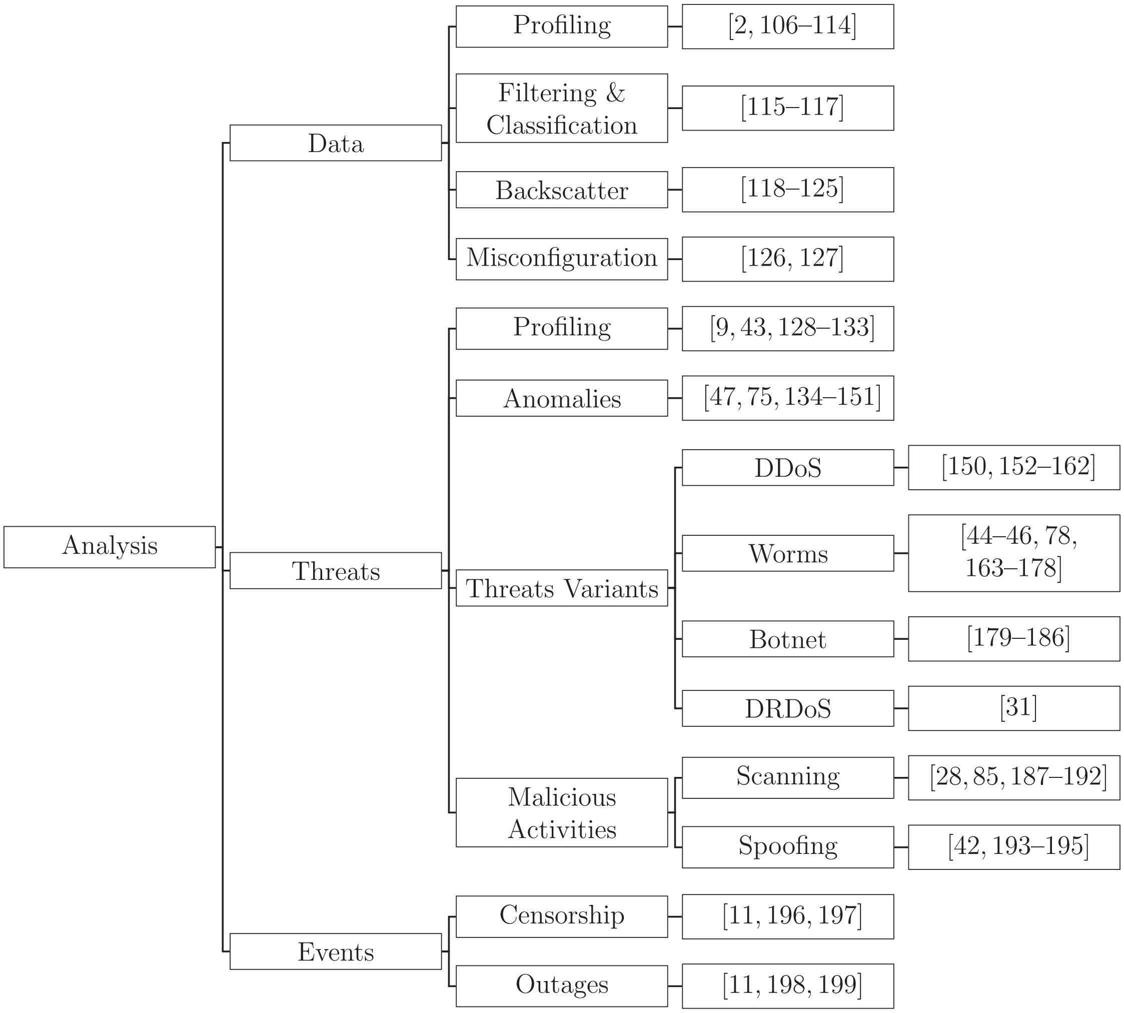

Figure 3.5: Analysis Research Taxonomy - Overview

on Microsoft Windows systems. Furthermore, Pang et al. [108] present a study of the broad characteristics of darknet. The authors develop filtering techniques and active responders to use in their monitoring process. They analyze both the characteristics of completely unsolicited traffic (passive analysis) and the details of traffic elicited by their active responses (activities analysis). Moreover, Shimoda et al. [109] propose a system to improve passive darknet monitoring. The proposed approach leverages active hosts with no effect on legitimate connections. This light-weight multi-dimensional IP/port analysis system enables TCP ports monitoring. In this context, Ford et al. [107] create the first IPv6 darknet. The aim of this work is to

Publications	Approach/Technique	Contribution	Tool/Project
[106]	Comparative Study - Packet Filtering	Exploring Data Across Five Different Darknet Sensors	TENET
[108]	Packet Filtering - Routing	Characterizing Darknet Data	iSink
[107]	IPv6 Packet Analysis - Routing	Creating the First IPv6 Darknet	Custom
[109]	Multi-Dimensional IP/Port Analysis	Proposing a System to Improve Darknet Monitoring	Custom
[111, 112]	Time Series - Principle Component Analysis	Discussing the Temporal and Spatial Correlations in Data	Custom
[110]	Packet Filtering	Inferring the Evolution of Internet Infrastructure	CAIDA
[2]	Time Series - Spatial Analysis	Discussing Topics Related to Darknet	Custom
[113]	DNS Analysis	Introducing the Concept of Dark DNS	honeydns
[114]	IPv6 Packet Analysis - Routing	Studying IPv6 Darknet Data	Custom
[200, 201]	Time Series	Studying Different Entropy Metrics	Custom - CAIDA

Table 3.7: Profiling Research Papers - Summary

compare between IPv6 and IPv4 darknet. The results showed that traffic targeting IPv6 darknet is minimal. Furthermore, Dainotti et al. [110] infer the evolution of Internet infrastructure. Instead of using active probing techniques, this technique leverages darknet traffic monitoring to provide some insights on the utilization of the Internet. The investigation touches the limited visibility of a unique observation point as well as the existence of IP spoofed addresses in data that can fake analysis results. The authors propose new techniques to remove spoofed packets and compare their results with methods that use active scans. Oberheide et al. [113] introduce the concept of dark DNS, which is based on the analysis of DNS queries found on darknet addresses. They also profile the DNS dark data collected from their sensor and discuss the implications of evading sensor through DNS reconnaissance. They further stress on the defense aspect using proactive measures when deploying darknet sensors through delegating reverse DNS authority in a proper manner. At the end, they introduce honeydns, which complements low-interactive and darknet sensors by providing DNS trap services. Finally, Czyz et al. [114] report a large study of IPv6 darknet data. Through the analysis of five large /12 network address space, the authors highlight the nature of the traffic and compare it with IPv4 data. The researchers also provide various case studies to show notable properties while analyzing darknet IPv4 and IPv6 data.

Furthermore, time series analysis techniques are also used to profile passive monitoring data. For example, Fukuda et al. [111] discuss the temporal and spatial correlations among piecewise unwanted traffic. The aim of their techniques is to determine whether they can estimate statistical properties of global unwanted traffic behavior from smaller darknet address blocks. They found that the fluctuation of darknet traffic was close to random compared to normal traffic. Moreover, the authors demonstrated that the TCP SYN traffic time series had a strong spatial correlation. On the contrary, for TCP SYNACK and UDP traffic time series, Fukuda et al. [112] confirmed that in this case they were less correlated. The authors stress the need for a more sophisticated classification of the UDP unwanted traffic. They further investigated the macroscopic behavior of unwanted traffic collected using a /18 darknet over one year period. In order to measure the complexity in network traffic, Riihijarvi et al. [200] study different entropy metrics. The generated metrics provide a better understanding of the traffic and help finding a new way to characterize the data. Moreover, the proposed technique uncovered structures on different traffic measurements and timescales. These authors extend their work to propose the use of multi-scale entropy analysis to characterize network traffic and spectrum usage. They showed that this technique can quantify complexity and predictability of analyzed traffic in widely various timescales. The results further showed that different entropy structures exist for different traffic traces such as time series and commonly-used traffic [201]. Last but not least, Wustrow et al. [2] discuss topics related to darknet. They pinpointed the rapid growth of Internet pollution that was out spacing the growth of productive network traffic. Furthermore, they noticed trends toward increasing SYN and decreasing SYN-ACK traffic. In addition, they examine several case studies in Internet address pollution and offer specific suggestions for filtering them.

Data Filtering & Classification

Data filtering and classification include the classification and filtering approaches of darknet data. These techniques are summarized in Table 3.8.

Publications	Approach/Technique	Contribution	Tool/Project
[116]	Relative Uncertainty Theory	Filtering Darknet Data	Custom
[115]	Classification Scheme	Composition of Darknet Data	Custom
[117]	Hybrid	Manual Identification and Automated Generation of Data	Custom

Table 3.8: Filtering & Classification Research Papers - Summary

Glatz et al. [115], for instance, analyzed a dataset that captured a significant amount of traffic to shed light on the composition of darknet towards large networks. The approach is based on a one-way traffic classifier. The authors found that such traffic constitutes the majority of all traffic in terms of flow and can be primarily attributed to malicious causes; however, it has declined since 2004 due to the relative decrease of scan traffic. Moreover, Wang et al. [116] propose a novel approach to filter darknet traffic. Their technique is based on relative uncertainty theory and is independent of configurations or building databases. The authors assume that data coming from regular users is relatively certain and not random. Furthermore, Cowie and Irwin [117] discuss the difficulties in generating training traffic for Artificial Intelligence (AI) analysis. The authors mention the problem in accurately labeling known incidents from darknet. Other factors related to this issue include the originality of data and the time involved. To address this problem, they work on two techniques, namely manual identification and automated generation. The first counts on heuristics for finding network incidents whereas the second considers building simulated data sets. They were able to construct a sample of an AI system out of this marked dataset.

Backscatter Data

Backscatter data is the reply packets sent to the darknet. Several factors can produce such scenario, such as DDoS victims replying to spoofed IP addresses and misconfiguration. Table 3.9 summarizes the works that leverage backscattered traffic to generate cyber insights. Under this category, the research contributions employ several techniques such as mathematical models, network routing, packet filtering, and visualization.

Publications	**Approach/Technique**	**Contribution**	**Tool/Project**
[125]	TCP Delay	Detecting Network Congestion	CAIDA
[121, 122]	Matching Pursuit (MP) Algorithm	Detecting Malicious Traffic	CAIDA
[118]	Bloom Filter	Enhancing Counting Bloom Filter's Hash Space	RSECBF - CAIDA
[120]	Distributed Stubs	Detecting Anomalies	DTRAB - CAIDA
[119]	Entropy-Based	Studying Entropy-based Anomaly Detection	CAIDA
[124]	Multi Connections	Detecting Anomalies	MCAD - CAIDA
[123]	Clustering	Extracting Traffic Signatures	PISA

Table 3.9: Backscatter Research Papers - Summary

For instance, Peng et al. [118] propose a Reconstruction based on Semantically Enhanced Counting Bloom Filter (RSECBF) algorithm to reveal the distribution of the main elements from semantically enhanced Counting Bloom Filter's hash space. The proposed algorithm deploys a specific technique, which directly selects certain bits from the primary string. The authors confirm the homogeneous hash strings and show the efficiency of the algorithm using real backscatter traces. Moreover, Rahmani et al. [119] study entropy-based anomaly detection through backscatter from darknet data. In particular, the authors try to understand the detection strength of using joint entropy analysis of many data distributions. The authors found statistical correlation between time series of IP flow number and collective traffic size. The approach was tested on backscattered data and led to more effective and accurate DDoS detection techniques. Moreover, Choras and Saganowski [121, 122] leverage backscatter data to propose an anomaly detection technique for recognizing malicious traffic. Using the correlation of parameters from different layers, the authors were able to detect unknown attacks with a low amount of false positives. The authors correlated signal-based and statistical features to enhance their technique. The proposed framework uses, for the first time, the Matching Pursuit (MP) algorithm [202] on network traffic. They found superior results to other IDSs that work on discrete wavelet transform. Similarly, Fadlullah et al. [120] detected anomalies through strategically distributed Monitoring Stubs (MSs). This work was able to categorize encrypted protocols. The MSs are designed to extract features and build normal behaviors. Based on deviations in traffic, the technique can differentiate between suspicious and benign traffic. After the detection process, MSs notify victims to trace-back the source of the attack and take necessary action.

He and Parameswaran [124] leverage backscatter data to propose a novel anomaly detection system based on multiple connections. The approach is considered faster than previous anomaly detection mechanisms. This Multiple Connection based Anomaly Detection (MCAD) system relies on the concept that attackers use similar connections to execute an attack. Hence, the algorithm tests for similarities within connections, and if the value is above a certain threshold, the connections are flagged as malicious. Over one million connections of backscatter traffic were tested in this work. MCAD was able to identify fifteen forms of connections, in which fourteen were fully detected while only one was detected with 66% accuracy. In addition, in order to detect congestion online, the authors in [125] propose a mechanism to detect congestion in network traffic by analyzing passive and aggregation links. The technique is based on delays in TCP data. The approach was tested on backscatter data and proved to be efficient. This technique is considered dynamic with fast detection capability. In an attempt to fingerprint malicious attacks, Chhabra et al. [123] propose PISA, a packet imprint in security attacks algorithm, for automatic extraction of traffic signatures. PISA has the capability to cluster flows based on similarity in packet information and generate signatures from clusters. This tool was tested on two weeks of backscatter data encompassing 100 million packets. The results inferred about 1744 signatures related to several malware including the Blaster worm.

Data Misconfiguration

Data misconfiguration is the act of incorrectly setting up a machine on a certain network. This section lists research works that leverage darknet to infer misconfiguration, errors and data management in network communications. Relevant contributions are shown in Table 3.10.

Publications	Approach/Technique	Contribution	Tool/Project
[126]	Probing - Routing	Reachability Analysis	Arbor Networks
[127]	Packet Filtering - Routing	Studying Trends of Network Misconfiguration	CAIDA

Table 3.10: Misconfiguration Research Papers - Summary

For instance, Francois et al. [127] demonstrate that darknet is a powerful tool in analyzing malicious network activities as well as network management. The authors present trends of network misconfiguration using darknet analysis. In practice, the results illustrated that deployed networks suffer from well-known errors and faulty configuration. Furthermore, Labovitz et al. [126] present a large study on the one-sided differences in Internet service provider reachability. The authors focus on darknet and the range of topology reachable to some providers but unreachable through one or more competitor networks. They present both active and passive measurements of differences between service providers' reachability. The goal is to discover the level to which commercial strategies, peering disputes, network failures, misconfiguration, and various malicious acts can lead to a partitioning of Internet topology. The results showed that the Internet was indeed partitioned and that darknet existed in a large amount (5% of Internet addresses). Moreover, the authors found that some prefixes were reachable only to specific providers. In addition, 70% of hosts responded to reachability tests and the majority of these devices were cable/ISDN pools and US military hosts.

3.2.2 Threat Analysis

One of the major elements in passive network monitoring is the extraction of insights on suspicious activities and threats on the Internet. Recall Figure 3.5, this section includes the research contributions in the following areas: threat profiling, anomalies, threats' variants and malicious activities.

Threat Profiling

Threat profiling includes the characterization (profiling) of darknet threats. Table 3.11 lists the threat profiling papers. Several techniques are used to profile darknet threats such as time series, statistics, and network routing.

Various researchers utilize time series and statistical methods to profile darknet threats. For instance, Harder et al. [128] study the statistical properties of class C darknet addresses for over three months. The authors found that the majority of the traffic is based on few IP sources and destination addresses. The study included a demonstration using many visualization techniques to represent darknet data and showed severe attacks such as DDoS and scanning activities. Using different techniques, such as power spectrum, inter-arrival time of packets and detrended

Publications	Approach/Technique	Contribution	Tool/Project
[43]	Broad-Spectrum	First to Investigate Trap-based Monitoring Systems	Custom
[59]	Packet Filtering	Representing the Infrastructure of Data Gathering	honeyd/WOMBAT
[128]	Time Series - Statistics - Power Spectrum	Studying the Statistical Properties of Darknet	Custom
[129]	Statistics	Presenting the Leurre.com Project	Leurre.com
[130]	Graph-based - Statistics	Proposing a Distributed Monitoring System	Custom
[131]	Time Series	Predicting Anomalies	DCMA
[132]	Change-Point - Data Mining	Analyzing Suspicious Behaviors	NICTER
[133]	Comparative Study and Correlation	Studying the Selection of Sources of Information	CAIDA ATLAS SANS DShield

Table 3.11: Threat Profiling Research Papers - Summary

fluctuation analysis of this data, the authors found small signs of long-range dependency within the analyzed traffic. Francois et al. [130] leverage statistical techniques to propose a distributed system that monitors threats using centrality of a graph and its time evolution. Furthermore, Holz [129] presents the leurre.com project and discusses the importance of collecting data from different locations and generating results based on correlation engines. The author highlights insights in terms of finding attack patterns and pinpointing root-causes of threats. Ohta et al. [131] uses time series analysis to study the possibility of predicting anomalous packets' behaviors by observing a small darknet address space. The researchers propose distributed cooperative monitoring architecture (DCMA) technique, which aims to probe and detect anomalous packets. The authors calculate the correlation strength of anomalous packets, observe the correlation strength when changing the sub-observation's size, and note the dependency of the correlation strength.

We further list contributions that utilize hybrid and custom techniques to characterize darknet threats. For example, Bellovin et al. [43] are among the first to investigate trap programs that search for attacks. Their work can also be the primary motivation that triggered the idea of darknet monitoring. A variety of pokes were found during their analysis. The authors believe that these attacks occured on many online sites without the administrators' knowledge. In this work, they also provide important security information to security operators on how the attackers were operating [9]. In addition, Inoue et al. [132] utilize NICTER to propose a novel method to analyze suspicious behaviors. The latter technique is based on the malware's external behavior. Their experiment is executed in a safe environment using virtual machines. Moreover, Dacier et al. [59] leverage WOMBAT to represent the infrastructure of data gathering. This project is based on an extended version of honeyd with SGNET [203]. In this experiment, the authors were able to observe the evolution an army of zombies. Their approach is found to be efficient to use for multidimensional analysis of events. The authors also shared some insights found when collecting malware (including zero-day) and described different stages of attacks. Finally, Berthier et al. [133] present a large and comparative study to help security operators in selecting sources of information. By comparing three different sources of security information including darknet dataset, the authors correlated attacks among different sources of data having various granularity.

Anomalies

Anomalies are defined by the acts of deviation from the normal network traffic pattern. This section provides a summary of the darknet-based research that targets the detection and mitigation of anomalies. Table 3.12 denotes these research publications. The major techniques are based on IDS, mining, clustering, and time series.

Publications	Approach/Technique	Contribution	Tool/Project
[137]	Packet Filtering - Routing - Data Mining	Proposing a Novel Application of Large-scale Monitoring	Nicter
[75]	Time Series - Mathematical Model	Monitoring Large-scale Security Threats	CAIDA
[147]	Opportunistic Measures	Uncovering Hidden Regions of the Internet	Custom
[148]	Automated Knowledge Discovery	Introducing Cliques	Cliques Leurre.com
[134]	Generic IDS - Firewall	Presenting an Empirical Analysis of Internet Intrusion	Custom
[47]	Time Series - Discrete Wavelet Transform	Observing Unknown Malicious Activities	Custom
[145]	Cardinality Variation	Analysing and Detecting Cyber Attacks	Custom
[146]	Poisson Statistical Process	Detecting Malware	IMS
[138]	Knowledge Discovery - Data Mining	Studying New Emerging Attack Phenomena	Honeyd Leurre.com
[141]	Context-Aware	Detecting and Mitigating Online Threats	Custom
[142]	IDS - Association Rule Mining	Characterizing Data and Investigating Threats	Custom
[143, 144]	Time Series - Sliding Window Cumulative Sum - Change Point	Automatic Recognizing Variations in Network Traffic	Custom
[139]	Time Series - Pattern Recognition - Clustering	Analyzing Attack Patterns	Honeyd leurre.com
[140]	Knowledge Discovery - Fuzzy Decision Making	Proposing and New Technique for Attack Attribution	Honeyd leurre.com
[135]	IDS - Hidden Markov	Describing an Adaptive NIDS with a Two-stage Architecture	Custom
[149]	Messaging Framework	Proposing a Framework for Real-time Analysis	Custom
[150]	Selective Pulling - Ratio-Based Algorithm	Proposing a System for Timely Business Intelligence and Decision Making	RTQ
[136]	IDS - Statistics	Exploring New Techniques to Leverage Darknet Monitoring	Honeyd
[151]	Hotspots	Defining Hotspots for Malware Detection	IMC

Table 3.12: Anomalies Detection and Mitigation Research Papers - Summary

First, several researchers leverage IDS systems to detect anomalies. For instance, Yegneswaran et al. [134] present a broad, empirical analysis of Internet intrusion activity using a large set of Network-based IDS, firewall logs and darknet data.

Their breakdown of scan types showed not only a large amount of worm propagation but also a substantial amount of scanning activities. To gain insights into the global nature of intrusions, the authors use their data to project the activity across the Internet. They also present a theoretic evaluation on the potential of using data shared between networks as a foundation for a distributed intrusion detection infrastructure. Furthermore, Karthick et al. [135] use probability to describe an adaptive network-based IDS with a two-stage architecture. The first stage includes a probabilistic classifier whereas the second uses a Hidden Markov Model to narrow down the attack source IPs. The proposed hybrid model was tested and showed good performance in detecting intrusions. For the purpose of providing situational awareness, Barford et al. [136] explore techniques that can be used to integrate trap-based monitoring data into daily monitoring systems. These techniques are based on IDS system and other statistical methods. The authors also discuss techniques that can detect whether an attack is purposely or incidentally targeting a victim as part of a larger attack. The analysis showed prevalence of different scanning techniques and useful information on trends, uniformity, coordination, and darknet-avoidance.

Second, several authors utilize mining and clustering techniques to learn about anomalies. For example, Inoue et al. [137] leverage resources from Nicter to propose a novel application of large-scale darknet monitoring in live networks. The technique investigates packets transmitted from inside networks instead of outside. In addition, Thonnard and Dacier [138] aim to generate insights on the method of operation of new emerging attack phenomena. To accomplish this goal, they have presented a multi-dimensional knowledge discovery and data (KDD) mining method. This technique extracts meaningful nuggets of knowledge and synthesizes those pieces of knowledge at different dimensional levels to create a concept that can best describe real-world phenomena. Furthermore, Thonnard et al. [139] present an analysis framework for discovering groups of attack traces having similar patterns. The authors extract knowledge of darknet data by discovering attack patterns via attack trace similarity, rather than a rigid signature. The results of their clustering method enabled the identification of activities of several worms and botnet in the collected traffic. In a similar work [140], the authors introduce a general analysis method to address the complex problem related to attack attribution. Their approach is based on a mixture of knowledge discovery and a fuzzy decision making process. By applying their technique on darknet attack traces, the researchers showed how to attribute and identify large-scale orchestrated cyber campaigns. Finally, in our work [142], we have characterized darknet data and investigated darknet threats. The aim is to study threats that are found on darknet and prioritize their severities. We further explored the inter-correlation of these threats by conducting association rule mining studies to generate association rules. Our technique extracts clusters of co-occurring malicious activities targeting certain victims. This contribution proved that some threats found on darknet are correlated. Furthermore, our technique provided intelligence about patterns within threats and allowed the interpretation of attack scenarios.

Third, the following group of authors uses time series techniques. Limthong et al. [47] applied Discrete Wavelet Transform (DWT) techniques for traffic signal decomposition and observed unknown malicious acts from darknet information. In particular, the authors focus on TCP SYNs, TCP SYN/ACKs and UDP packets based on three time intervals. The purpose of this work is to show the importance of time series wavelet methods in finding insights about malicious communications on darknet. In addition, Ahmed et al. [143, 144] leverage time series techniques and the dynamic sliding window cumulative sum (CUSUM) algorithm to automatically recognize nested changes in network traffic and detect any number of these changes. This automatic detection approach can identify both the beginning and the end of abnormal changes.

Finally, several hybrid and custom techniques are used to detect and mitigate anomalies. For example, Chen et al. [145] focus on the analysis and inference of cyber attacks through a technique based on the changes in the cardinality of the attack traces. The approach develops a nonparametric error-bound scheme with the capability to detect cyber attacks through a centralized data center of multi-monitoring sensors. This scheme uses small space and constant processing time, which allow the system to operate in near real time. In addition, a statistical approach is used by Soltani et al. [146] to detect malware on darknet traffic. The authors introduce the Piecewise Poisson process Model (PPM) and check the rate of traffic to detect malware outbreaks. The researchers then implement a regression model that can be used to characterize changes in the PPM data rates. In addition, Moore et al. [75] leverage the analysis of darknet traffic to monitor large-scale security threats. They showed a trend in cyber attacks based on a period of over two years. Moreover, these authors study the relation between the detection ability and size of these sensors, profile precision in detecting duration and rate of an attack, and discuss good practices in darknet deployment. Furthermore, Casado et al. [147] propose opportunistic measures from spurious network traffic (such as darknet) to uncover hidden regions of the Internet. The authors identify such sources and demonstrate their possible use in providing efficient statistical data. In addition, Pouget et al. [148] introduce an automated knowledge discovery technique called Cliques. The Cliques methodology provides insights on how attacks occur and potentially identifies the source behind them. The authors used the proposed methodology and found useful data about similarities in the method of operation of many potentially unrelated malicious tools. In addition, Hunter et al. [149] propose a framework for real-time analysis of darknet and honeypot data. The technique uncovers several malicious behaviors. In order to collect data, the authors develop an automated reconnaissance (AR) framework that works in both passive and active modes. The authors utilize several features to identify malicious users such as OS name, targeted service, location and services operating on the adversary. Gupta et al. [150] propose a ratio threshold queries

(RTQs) system that can be used for timely business intelligence and near real time decision making. For instance, the system can defend against malicious attacks on the Internet such as DDoS when the ratio of queries surpasses a certain threshold. The system further uses selective pulling techniques for inferring extra sources. In addition, Sinha et al. [141] investigate techniques in detecting and mitigating online threats via the context available in network, environment and host. The authors explain the context concept which is based on three main properties: vulnerability profile, attack surface, and usage model. The authors leverage ten years of experience to prove the efficiency of the approach in enhancing security techniques. Last but not least, Cooke et al. [151] define hotspots as the root cause of non-uniformity in self-propagating malware. In this work, the authors claim that two main factors are behind its existence, namely, the algorithmic and environmental factors. Using eleven sensors located at different addresses around the Internet, they measured the impact of these factors on the propagation of worms and bots (or zombies). Based on this idea, the authors simulated the outbreak of new threats with hotspots and demonstrated the effect of the aforementioned factors on the visibility of monitors and hence the efficiency of detecting new threats.

Threats Variants

Threats variants include various threats. We list in this section the threats that can be detected through the analysis of darknet data, namely, DDoS, worms, botnets and DRDoS.

Distributed Denial of Service attack is one of the most severe cyber threats. Denial of Service (DoS) attacks are characterized by an explicit attempt to prevent the legitimate use of a service. Table 3.13 summarizes darknet-based DDoS research papers. Below is an overview of these studies. Some techniques include mathematical models, network routing and packet filtering.

Publications	Approach/Technique	Contribution	Tool/Project
[204, 205]	Chi-Square Statistics	Detection	CAIDA
[152]	Identifier/Location Separation	Prevention	Custom
[206]	Greedy Algorithm	Detection	Custom
[150]	Greedy Algorithm	Detection	Custom
[153]	Stream-Based Processing	Prevention and Mitigation	STONE
[154]	Adaptive and Hybrid Neuro-fuzzy	Detection	NFBoost
[155, 156]	Traffic Analysis - MIB	Detection and Mitigation	D2M2
[157, 157]	Flow-Based Algorithm - Data Mining - Time Series	Prediction	Custom
[159]	Data Correlation	Detection and Mitigation	OADS
[160]	Total Variation Distance	Detection	Custom
[161]	Flow-level - Reputation-Based	Prevention and Mitigation	TrustGuard
[162]	Change Point	Detection	Custom

Table 3.13: DDoS Research Papers - Summary

First, the following publications leverage mathematical and statistical models for generating DDoS insights through darknet analysis. For instance, Andrysiak et al. [206] focus on detecting DDoS threats using greedy algorithms. More specifically, the approach uses Matching Pursuit algorithms, which look into best matching projections of multidimensional dataset. Similarly, Gupta et al. [150] focus on the analysis of backscatter and MAWI data [207] to detect DDoS by means of greedy algorithms. The approach is based on several matching pursuit algorithms. In addition, Arun et al. [154] propose NFBoost, an adaptive and hybrid neuro-fuzzy approach to detect DDoS attacks. The approach combines various classifier outputs and cost strategy minimization technique for classification determination. The approach was tested on real DDoS traces and trained with publicly available dataset.

Furthermore, the evaluation was based on two metrics, namely the detection accuracy and cost. In our work [157, 158], we have propose an approach to predict, within minutes, certain DDoS and their attacks features; namely, intensity/rate and size. The aim is to forecast the future short term trend of DDoS attacks. The analysis is based on darknet data and the attack traces are tested for predictability using a time series approach prior to predicting. In addition, Rahmani et al. [160] propose a two-stage DDoS detection approach based on the breaks in the connection size distribution. To achieve this goal, the authors employ a total variation distance technique to calculate the horizontal and vertical similarity between flows. The approach detects high- and low-rate DDoS attacks. Furthermore, Abouzakhar et al. [204] present a network-based system for anomaly detection using chi-square statistics. This technique is a robust multivariate anomaly detection method with minimum computation cost. The objective of this method is to reduce the limitation of intrusion detection and network forensics. In an extended work [205], the same authors developed patterns for intrusion detection based on data mining techniques and Fuzzy algorithm. This Association Rule Mining-based (ARM-based) detection technique was successfully tested on real DDoS data. They further presented an enhanced Fuzzy ARM matrix for mining and associating rules. This hybrid approach can improve the efficiency of anomaly detection.

Second, other group of researchers tackle IP filtering and network routing techniques to investigate DDoS. For instance, Luo et al. [152] apply the identifier/location separation technique, a mechanism to solve the issue of routing scalability on the Internet to prevent distributed DDoS attacks. The proposed approach hardens the security to control machines (i.e., controlling infected machines through a botnet). This approach was evaluated using real DDoS traffic and showed promising results. Furthermore, a change point technique coupled with an analysis of source IP addresses are used by Ahmed et al. [162] to detect high-rate flooding attacks. The authors use a proof of concept development of the proposed methodology and show the efficient representation of pre-onset IP addresses that can also be used for threat mitigation.

Finally, other DDoS detection and mitigation techniques are used such as Chen et al. [153] who introduce STONE, a stream-based framework designed to defend against DDoS attacks. The STONE is a hybrid and scalable system that leverages anomaly-based inference and mitigation. The system operates through continuous data streaming queries to maintain data processing. The approach is also useful in the case of flash (high speed) events and operates in a priority-based fashion. STONE is built on top of StreamCloud, which is an elastic parallel-distributed stream processing engine. Additionally, Bhatia et al. [155, 156] propose a model to detect and mitigate DDoS attacks. The model uses an MIB (Management Information Base) server load and network traffic analysis to detect DDoS attacks from various network layers. The proposed model has the capability to distinguish DDoS from flash events. Further on DDoS, Feitosa et al. [159] also propose an approach to detect and mitigate DDoS attacks. They present the specification of a new orchestration-based technique to infer and mitigate threats. The proposed approach is based on a framework that coordinates alerts and events, infers threats, and consequently chooses the ultimate action. The authors generate rules and infer attacks with a greater degree of certainty than simple anomaly detectors. Finally, Liu et al. [161] examine drawbacks of existing DDoS defense schemes and propose a credit-based defense system. This approach focuses on the diversity in size of the attack; the less diverse the attack flow, the smaller credit it gets. The DDoS attacks were found to accumulate less credit as they naturally have low diversity in their traffic. This mechanism was able to identify the characteristics of micro and macro DDoS attackers and victims.

Worms are malicious codes known to infect and propagate in a rapid manner. We list in this section the contributions related to computer worms via darknet data

Publications	Approach/Technique	Tool/Project	Worm
[163]	Packet Filtering - Routing	CAIDA	Code Red
[44, 164]	Packet Filtering - Routing	CAIDA	Slammer/Sapphire
[165]	ICMP Packet Analysis - Simulation	Custom	
[166]	UDP Packet Analysis - Routing - Simulation	CAIDA	Slammer
[45]	Routing - Time Series	CAIDA	Witty
[167]	Distributed Monitoring Sensors	Custom	Blaster - Slammer - Code Red II
[46]	Packet Filtering - Routing	IMS - Arbor	Blaster
[168]	Analytic Modeling - Simulation	Custom	
[169]	Packet Filtering - Routing	CAIDA & iSink	Witty
[170]	Time Series	CAIDA	Witty
[171, 178]	Kalman Filter - Simulation	CAIDA	Code Red - SQL Slammer - Blaster
[172]	Time Series - Clustering	Honeyd/Leurre.com	
[173]	Flow-Based - Clustering	Custom	Welchi - Slammer - Opasoft - Messenger
[78]	Micro & Macro Analysis	NICTER	W32.Downadup
[174, 175]	Maximum Likelihood & Regression	Custom	Code Red
[176]	Packet Filtering & Source OS	Custom	Conficker
[177]	Bloom Filter - Packet Filtering	Custom	

Table 3.14: Worm Investigation Research Papers - Summary

analysis. Table 3.14 summarizes these contributions. The majority of techniques are focused on packet analysis, routing, mathematical models, statistics and time series.

Moore et al. [163] analyze the Code-Red worm. Primarily, the authors showed the spread of this worm based on its deactivation and infection. The worm infection rate peaked at 2000 hosts per minute. Subsequently, the authors geographically located and measured the population of the worm and checked affected ISPs and top level domains. Additionally, Moore et al. [44, 164] study the Slammer worm through darknet analysis. In particular, they showed how this worm selects its victims and explained the reasons behind its fast propagation. They further discussed the pitfalls of the worm's author which aid in its discovery. In addition, they executed several related measures, geographically located the worm's victims, and listed the geographic distribution of the worm. Finally, the authors highlighted the impact of the Slammer worm on Internet operations. Likewise, Berk et al. [165] present a technique to identify worm spread after a short period of time. This method detected worm spread only when 10% of the victims are infected and with a detection performance achieved with sensor covering only 1% to 2% of the monitored space. This automated system is based on ICMP unreachable messages. This proposed methodology examines worms and presents simulation results that measure the detection speed of active hosts. Also, Staniford et al. [166] investigate UDP-based worms. The authors simulate the Slammer worm, adjust its latency measurements and monitor its packet delivery rates. The results showed that 95% of 1 million vulnerable hosts can be infected in only 510 milliseconds, whereas another TCP based service can be 95% saturated within 1.3 seconds. To avoid worm containment techniques, the authors suggest that flash worms should reduce their speed and use deeper spread trees. Furthermore, the proposed approach includes defense mechanisms to detect flash worms. In addition, Shannon and Moore [45] study the Witty worm, which targets a buffer overflow flaw in many firewall products having Internet Security Systems. The authors shared a general view of the worm's spread, its victims and features. Similarly, Kumar et al. [169] analyze the propagation of the Witty worm. The authors exploit the structure of the code including its pseudo-random number generation function. Using limited darknet data, the researchers were able to mine individual packets' rate of infection prior to loss, corrected noise generated by the worm, and disclosed the worm's failure to reach all potential victims. Furthermore, these scientists explored the complete attack infection scenario tree and uncovered a target on a US military base. Furthermore, Abu Rajab et al. [170] utilize darknet data to infer the sequence of worms infection. The authors test the reliability and effectiveness of their proposed technique independent of scanning rate, vulnerable population and the sensor size. These authors measured the accuracy of this time series-based methodology, which reaches 80% after a few hundred initial infected machines. This technique further provided insights into the characteristics of the hit-list. Last but not least, Zou et al. [171, 178] investigate worms in two separate works. First, the authors propose several algorithms (i.e., Kalman filter) that effectively detect worm presence and its corresponding sensors. Second, they showed that they can predict the overall vulnerable population size of a uniform-scan such as Code Red. They further accurately estimated the infection size based on the analyzed data.

Moreover, Bailey et al. [46] use a /8 darknet network from the IMS project to describe observations of the Blaster worm since its beginning in 2003. The authors explain how they measure its propagation, attack scenario, worm characteristics, life cycle in 2003, and persistence in 2004. Furthermore, Richardson et al. [168] examine how darknet affected the ability of global scanning worm detectors. They propose statistical models of darknet and combine them with random constant spread model of worm propagation to calculate the probability that a worm detector would be able to raise an alarm. Through their analysis, the authors concluded that global scanning worm detectors are not a viable long-term strategy for detecting worms in early stages. Additionally, Cooke et al. [167] try to understand non-uniformity in worms' behavior. Using a large darknet data rich with Blaster, Slammer and Code Red II infections, the authors analyzed and discovered three bias in malware behavior. More on worms detection, Pham et al. [172] tackle the problem of discovering multi-headed worms in the context of a larger dataset. Based on a 15 month of data, the researchers were able to confirm the existence of multi-headed worms and provided insights on worm behaviors. Kanda et al. [173] believe that worm-infected machine traffic characteristics are distinguishable from regular machines. They state that the difference in traffic between benign and malicious traffic can be classified by k-means clustering. Based on the volume of data, they also found that the proposed metric can isolate malicious traffic which has a small influence. Furthermore, Eto et al. [78] proposed an approach to understand the intentions of attackers and to have a comprehensive look of online threats. With focus on the W32.Downadup worm, the latter researchers found that 60% of their darknet attacking hosts are related to the above-mentioned malware. The authors also validated their findings with 86.18% accuracy using correlation analysis. Furthermore, Wang et al. [174, 175] estimate the temporal features of worms through simulation and analysis of darknet traffic. They propose several methods to detect the time of infection in order to rebuild the worm infection pattern. They leveraged this inference as a detection mechanism and estimate the detection error for various estimators. In addition, Irwin [176] studied worms in general and Conficker in particular. The author discussed the analysis of 16 million related darknet packets targeting port 445/tcp using a /24 address block. He further provided an overview and characterization of the collected data, including size and time to live (TTL) value analysis. This work pinpointed a flaw in the Conficker scanning algorithm [176]. Finally, the author located geographically the highly targeted victims based on region and numerical proximity. Finally, in an attempt to identify the location of worms binaries and stop their spread, Chen et al. [177] use the flexibility and high performance of network processors. The proposed inspection engine is built on top of an advanced network processor. The work includes testing and evaluating procedures to improve the performance of the proposed technique on real darknet data. The authors made the tool available for the anti-worm research community.

Botnet is a platform for adversaries to generate large-scale and distributed cyber attacks. We list below the research works that leverage passive monitoring to investigate botnet activities. Table 3.15 summarizes these publications. Contributions are divided into several techniques, mainly, trap-based monitors, clustering and correlation.

Publications	Approach/Technique	Contribution	Tool/Project
[179]	Diurnal Shaping Functions	Studying Botnet Spread Dynamics	Honeyd
[180]	Time Series	Tracking Botnet Activities	Honeyd/Leurre.com
[181]	Hybrid	Designing a Hybrid P2P Botnet	Custom
[182]	Data Correlation	Outlining the Genesis and Structure of Zombies and Botnet	IMS
[183]	Cross Cluster Correlation	Presenting a Platform for Botnet Detection	BotMiner
[184]	DNS-based Blackhole	Fingerprinting Botnet Activities Using a Non-interactive Approach	Custom
[185]	Spam Sinkhole	Studying Spammers' Behavior	Custom
[186]	IDS Correlation	Botnet Infection Detection	BotHunter

Table 3.15: Botnet Research Papers - Summary

First, Dagon et al. [179] study how time and location affect botnet spread dynamics. They create a diurnal propagation model that uses shaping functions to capture regional variations in online vulnerable populations. The model aims at comparing propagation rates for different botnets, prioritizing response and predicting future botnet infections. The authors found that time zones play an important role in botnet growth dynamics, and that factors such as time of release are important to short term spread rates. For data collection and validation, the authors used several tools including Tarpit [26]. The researchers demonstrated that their model is more accurate than the previous ones and that it accurately predicts botnet population growth. Furthermore, Ramachandran et al. [184] perform a counter-intelligence passive monitoring of DNS trap to infer botnets' activities without interacting with them. The authors were able to identify scanning activities performed by botmasters and suggested early bot detection techniques. Ramachandran et al. [185] further study the behavior of spammers through the analysis of a 17 month period of traffic flows to spam trap.

Second, Cooke et al. [182] outline the genesis and structure of zombies and botnet. The authors monitor command and control (C&C) and Internet Relay Chat (IRC) communication. By correlating security information from multiple sources, the authors elaborate on their botnet detection strategy. Additionally, Gu et al. [186] present a new strategy for network monitoring, which aims at inferring the infection and the coordination dialog of a successful malware infection. Through the analysis of a `/17` unused address space, the authors introduce BotHunter as an application to track the flows between internal and external entities. Using real network traces, the authors further evaluate the effectiveness of the project in detecting a variety of real-world botnets with low false positive rates. In a similar work, Gu et al. [183] present a general botnet detection framework called BotMiner. The authors started their investigation from essential botnet properties such as bots communication with C&C servers/peers. The technique uses cross cluster correlation to identify bots that share common malicious network patterns. This clustering methodology adopts many filters which include one-way traffic extraction such as scanning activity through uncompleted communication.

Other researchers such as Pham and Dacier [180] demonstrate how to track botnet armies of zombies to characterize their lifetime and size. First, they propose a time series technique to identify attack events in a large dataset of traces. Second, they identified long-living armies of zombies. Third, they showed the importance of selecting the observation viewpoint when trying to group such traces for analysis purposes. Last but not least, Wang et al. [181] present the design of an advanced hybrid P2P botnet. The system uses various features such as robust network connectivity, individualized encryption and control traffic dispersion, etc. To defend against such a botnet, the authors elaborate on various approaches including analysis via darknet space. In this context, the researches discover that if the darknet can capture 200 copies of peer lists, network security defenders will be able to know more than 95% of bots used in the peer-list updating procedure.

Distributed Reflection Denial of Service attack is also known as amplification threat. This is a well known practice of a DDoS, in which malicious users abuse publically reachable servers to overwhelm a victim with amplified reply traffic [208, 209]. The technique consists of an invader directing a query to an open server having the source IP spoofed to be the victim's address. Subsequently, all server responses will be sent to the targeted victim. In order to have a high impact on the victim, the attackers leverage requests with large size replies, and hence increase the amplification of the attack. Moreover, in order to increase the size of the attack with little effort, attackers use botnet to synchronize an army of bots and order them to send the requests. In recent research, DRDoS [33] activities are found to abuse several applications running on top of TCP [210] and UDP [32]. In our previous work [31], we have proposed a novel approach to infer and characterize large-scale DNS-based DRDoS activities through the darknet space. Complementary to the pioneer work on inferring DDoS victims using backscattered traffic [30], the proposed approach leverages DNS queries (non backscattered) that seek open DNS resolvers to execute the attack. The approach uncovered traces from the largest DRDoS attack of March 2013 against Spamhaus [211]. More on our DRDoS analysis is presented in Chapter 6.

Malicious Activities

Malicious activities consist mainly of two parts, namely, scanning and spoofing.

Scanning or reconnaissance activities are the first step in a cyber attack life cycle. In a typical attack scenario, adversaries execute a scan activity to search for vulnerabilities online before launching an attack on the vulnerable victim(s). Table 3.16 summarizes related research publications. The techniques are mainly based on time series and statistical models, in addition to network routing and packet analysis.

Publications	Approach/Technique	Contribution	Tool/Project
[187, 188]	Time Series - Statistics - IDS	Inferring Scanning Behavior	Custom
[85]	Spectrum Analysis	Extracting Malware Feature	SPADE
[28, 190]	Packet Filtering - Routing	Analyzing a World-wide VoIP SIP Scanning Campaign	CAIDA
[189, 192]	Statistics - Time Series	Proposing a General Framework to Extract Global Botnet Events	honeyd
[191]	White Hole	Defeating Malicious Probing Activities	Dark Oracle

Table 3.16: Scanning Research Papers - Summary

The first group leverages time series and statistical models to investigate cyber activities on darknet. For instance, Bou-Harb et al. [187, 212] attempt to infer scanning or probing activities and identify the technique used to perform such probing. The approach, which is based on various statistical and probabilistic techniques, tries to identify the machinery of the scan. The analysis is done on large darknet data and shows promising results. The same authors propose an approach to detect and cluster cyber attacks targeting corporate networks. They evaluated the approach and found promising results when compared with the mostly used NIDS (snort) [188]. Furthermore, Eto et al. [85] focus on the oscillations of the destination IP addresses of scan packets to propose the concept of malware feature extraction. They implemented and evaluated a distinct analysis method dubbed as SPADE. The technique applies a spectrum analysis methodology to realize a fundamental goal, which is to grasp the general trend of malware propagation from only scan data. Through several evaluations, the authors show that SPADE successfully extract and distinguish malware features. Additionally, Li et al. [189] propose a general framework to extract botnet global scanning events. Using honeyd, where half of the sensors are dark, the authors analyze one year of data from a large research institution to study six different botnet scanning characteristics. Based on scanning techniques, the researchers distinguish two botnet arrival/departure patterns. The authors study the scan behavior and differentiate between exponential and linear distributions. The result was affected by the randomness of scanning activities and the high range of scans, which cross the sensor IP space. In a relevant work, the authors investigate probing events of botnet. The discussed techniques are suitable for users who deploy darknet. The goal is to implement techniques that can help understand the strategy and purpose of the distributed probing events on the local network. Moreover, through the local view of sensors, the researchers designed the scheme of scanning activities, cross-validated their findings with DShield data and showed promising precision [192].

The second group leverage network routing techniques. For example, Dainotti et al. [28] present the measurement and analysis of a 12-day world-wide cyber scanning campaign targeting VoIP (SIP) servers. The discovery has occurred while analyzing some large-scale probing events [190]. Their analysis is based on their collected data using a `/8` dark IP address block. The authors note that the SIP scanning campaign involved approximately 3 million distinct source addresses (scanning bots), generated around 20 million probes, and targeted roughly 14.5 million destinations. For illustration purposes, the authors created a world map animation of the scanning campaign. Finally, Gu et al. [191] introduce a technique to counter scanning propagation. They propose the use of several components exploiting white hole networks, which are systems that co-occupy populated network segments to mislead and defeat malicious probing activities. Among these components, the authors use an address mapper that actively gathers and updates the unused IP/port segment of the network that the white hole can occupy. The white hole technique can deter, slow down and halt the spread of critical scanning malware. The authors demonstrate the effectiveness of their approach by using analytical reasoning and simulations using real trace and address distribution data. They further prove the success of their work even when applied to small darknet address blocks.

Spoofing is a technique to fake the identify of adversaries. Table 3.17 summarizes the related works that leverage darknet data. The techniques employ packet analysis and are divided into two categories.

Publications	**Approach/Technique**	**Tool/Project**
[193]	TTL Fields & Statistics	NICT
[194]	TTL & Identification Fields	Custom
[195]	ICMP Packets - Classification	Custom
[42]	ICMP Packets	CAIDA

Table 3.17: Spoofing Investigation Research Papers - Summary

The first group of authors leverage TTL values to investigate spoofing activities. For instance, Eto et al. [193] propose an inspection method focusing on the TTL field of each packet in order to statistically extract spoofed IP packets from traffic observed by darknet. They also provide an analysis engine against network attacks. Through an empirical evaluation, the authors found that at most 1.26% of spoofed packets exist in the darknet traffic. Similarly, Ohta et al. [194] propose an approach for detecting spoofed packets using the TTL and identification field frame values. The latter approach is based on time series analysis coupled with a statistical methodology. To validate the proposed approach, the authors used two darknet samples. They claimed that their method can extract a number of plausible spoofing packets from real darknet traces.

The second group of researchers uses ICMP packets to classify and trace-back spoofing activities. For example, Bi et al. [195] characterize spoofing attacks on the Internet. They classify address spoofing into six classes based on the position of the node being spoofed. This work also presents a trace-back mechanism to identify the origin of DDoS source based on the ICMP packets found on darknet. The results showed that attackers mostly use HTTP and HTTPS on top of TCP to execute their attacks. Last but not least, Yao et al. [42] present an Internet-scale Passive IP Trace-back mechanism that allows the tracking of the origin of anonymous traffic.

A developed Internet route model is sequentially used to aid in reconstructing the attack path. The researchers applied their technique to darknet data and found that the proposed mechanism can construct a trace tree from at least one intermediate router in 55.4% of the spoofing attacks, and can construct a tree from at least 10 routers in 23.4% of attacks.

3.2.3 Events

We list below the cyber events that are extracted through the monitoring of darknet. Table 3.18 provides a summary of these publications. The majority of the works leverage packet filtering and analysis to extract insights on events such as network outages, censorship, etc.

Publications	Approach/Technique	Contribution	Tool/Project
[199]	ICMP Probes	Proposing an Outage Detection Platform	Trinocular
[11]	Packet Filtering - Routing	Studying Darknet Events During Natural Phenomena	CAIDA
[196]	Packet Filtering - Routing	Studying Internet Censorship and Disruption	CAIDA
[197]	Packet Filtering - Routing	Exploring Internet Service Interruption	Custom
[198]	Packet Loss	Studying the Causes of Macroscopic Online Disruptions	CAIDA

Table 3.18: Events Research Papers - Summary

For instance, Quan et al. [199] propose Trinocular, an outage detection platform that uses ICMP probes which target darknet space. This system helps in understanding the reliability of edge networks and has the capability to provide precised indicator on outage period in terms of time and date. The approach leads to more accurate (fewer false conclusions) results in comparison to the best available techniques. Furthermore, Dainotti et al. [11] study darknet during two natural phenomena: country-level censorship and two recent earthquakes. For country-level outages, the authors note that these events are stunningly visible using darknet instrumentation, and in conjunction with other sources of data, this can reveal information about how censorship is being implemented over time. The authors also examine the number of distinct source IP addresses in darknet. They further study how the ratio of this number, before and after the earthquakes, varies by distance from the epicenters. It is shown that some graphs illustrated significant differences before and after the events, while other graphs showed more subtle differences. Similarly, the authors in [196] analyze episodes of disruptions caused by Internet censorship in two countries. Their analysis rely on multiple sources of large-scale data, including Internet registries files, Internet routing information, and darknet data. The authors were able to pinpoint the forms of Internet access disruptions, which were implemented in a given region over time. Among other insights, the authors detected Libya's attempts to test firewall-based blocking before executing aggressive external routing-based disconnection. The researchers claim that their methodology can be used, in an automated fashion, to detect outages or similar macroscopic events in other geographic or topological regions. Furthermore, Bailey et al. [197] leverage Internet routing, backbone traffic and darknet data to explore different infrastructure-based works to interrupt Internet services. The authors focused on the risks of this long-term Internet evolution based on several realistic events, such as WikiLeaks DDoS, China Facebook filtering, Iran elections and Egypt Internet outages [197]. Finally, Benson et al. [198] extend their disruption of Internet connectivity analysis to study the causes of macroscopic online disruptions. The authors propose metrics for inferring loss of packets in link congestion through AS analysis. This work listed three case studies to show how the approach can be used to identify and characterize large-scale outages.

3.2.4 Summary

Section 3.2 provided a taxonomy of several elements in the analysis process of darknet traffic, namely, data, threats, and events. Profiling darknet data allowed researchers to understand the nature of its traffic. Moreover, darknet was mainly designed to infer threats and malicious activities. Therefore, the analysis of darknet data in general and the threat analysis in particular, represented the largest part of this survey. From this section, we can conclude the following:

- A study in 2001 shows that darknet sensors occupy 5% of the whole IPv4 address space [126]. An up-to-date study is needed to approximate the current size of darknet.

- Various data analysis techniques are leveraging darknet traffic. The majority of studies tackle the IPv4 address space whereas less than 1% investigate IPv6 darknet.

- Packet analysis, network routing, statistics and time series techniques are the mostly used in darknet analysis.

- Filtering misconfiguration packets is still not thoroughly investigated and is still a gray area that requires more attention from the research community.

- Worms and scanning activities are the most common threats that can be found on the darknet.

- Code Red and Slammer/Sapphire are the most analyzed worms on the darknet due to their large-scale infection and propagation mechanisms.

- CAIDA data is the most widely used by researchers to investigate worms and other malicious activities.

- Denial of Service attacks are the most severe threats that are extracted from the analysis of darknet data.

- Botnet investigation is considered challenging through monitoring solely darknet traffic. The reason behind this is that darknet considers passive monitoring only. Therefore, other interactive techniques such as honeypots can be used in parallel with darknet to enhance botnet investigation.

- Nowadays, DRDoS are the largest cyber threats reaching a peak of 400 Gbps in 2014. DRDoS activities can also be measured by analyzing darknet data. Less than 1% of the research tackled this promising area of study.

- Due to the nature of darknet, which is based on passive monitoring, and the inter-activities in botnet systems, very few researchers were able to link botnet research to darknet analysis. In addition, due to reflection attacks, which have risen in the past couple years, several researchers were unaware of the importance of darknet in investigating such reflection activities. Therefore, botnet and DRDoS activities require more attention from the darknet research community.

- Differentiating between scanning and DRDoS is still partially a difficult problem due to the fact that both leverage scan-based techniques to operate. Scanning activities probe the Internet to collect information, whereas reflection attacks generate scan-based requests to redirect amplified reply traffic to victim.

- Scanning and spoofing are not threats but malicious activities that adversaries utilize to acquire information or hide identities respectively. More research has been done on scanning.

- Packet analysis is the only technique used on darknet data to investigate spoofing activities. This method includes inspecting ICMP packets and TTL values. Less than 2% of research has been done on spoofing and darknet. Therefore, spoofing is still a severe malicious activity that needs more attention from the security research community.

- Darknet can be used to check Internet policies due to certain events such as political, or geophysical, among others. For instance, the variation in the amount of darknet traffic generated, before and after a censorship policy, could allow researchers to assess the failure-to-success ratio of initiating this policy. During our study, we have found that analyzing darknet traffic upon worldwide events is the most recent.

The next section is the last part of our darknet taxonomy. The latter includes a state-of-the-art study of darknet visualization tools and techniques.

3.3 Darknet Visualization

Last but not least, we survey the literature and elaborate on the usage of darknet traffic in detecting malicious activities by exploiting visualization techniques and tools. The taxonomy of the visualization-based research works is shown in Figure 3.6. Furthermore, Table 3.19 summarizes these publications.

Le et al. [213] propose a novel approach to infer malicious network traffic based on graph theory concepts such as degree distribution, maximum degree and distance measures. The authors model the network traffic using the traffic dispersion graphs (TDG) technique [213]. As such, they analyze the differences of TDG graphs in time series to detect malicious activities and introduce a technique to identify attack patterns. The approach was validated using real network traces. Similarly, Joslyn et al. [214] propose a new technique to facilitate and visualize large-scale data. The graph-based approach leverages network routing databases. The authors described and presented real use cases in two graph-oriented query languages. This hybrid approach presents a new class of graph-relational analysis. In another visualization contribution, Krasser et al. [215] build a network traffic visualization system capable of both real-time and forensic data analysis. They aim to complement manual and

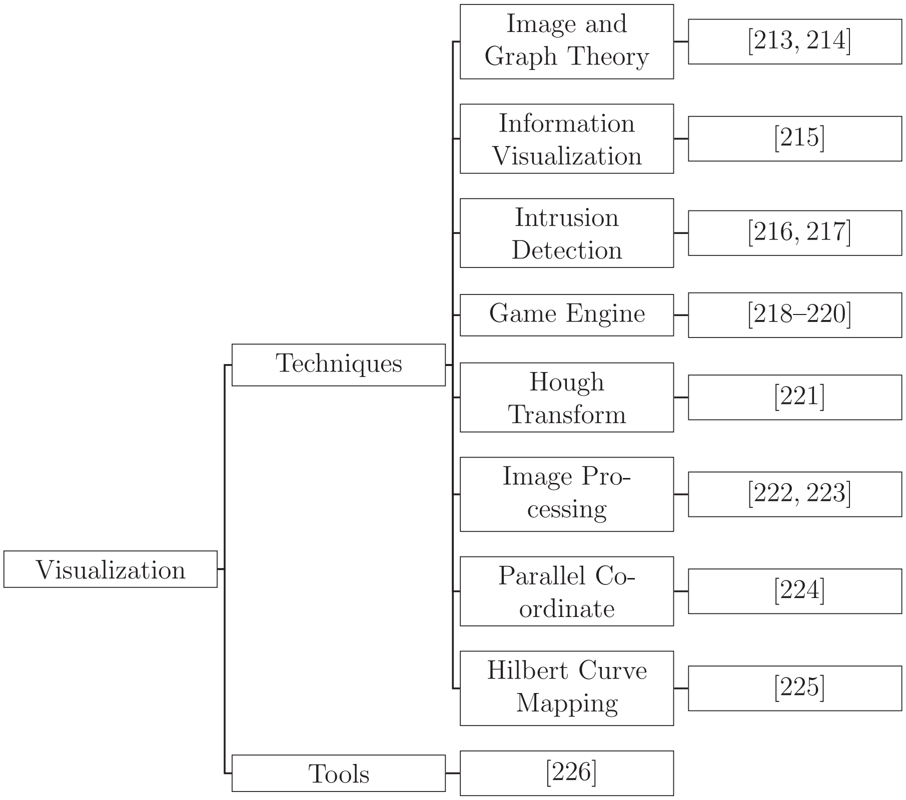

Figure 3.6: Visualization Research Taxonomy - Overview

automated analysis of network traffic by applying effective information visualization techniques in order to decrease the ratio of false positives and false negatives. Using link analysis and parallel coordinate plots with time sequence animation, the authors examine various dimensions that provide insights into both legitimate and malicious network activity. To validate the system operation, they used a dataset from five large-scale botnet traffic collected using darknet. Their results indicated that the system provides the capability to rapidly scan large dataset of network traffic for malicious activity despite visual noise. Moreover, Fontugne et al. [222] propose an approach for detecting traffic anomalies based on pattern recognition. The authors take advantage of graphical representations to break down the dimensions of network traffic. They further map network traffic data into snapshots rather than traditional time series. Moreover, these researchers identify unusual distributions

Publications	Approach/Technique	Contribution	Tool/Project
[214]	Graph-Based	Facilitating and Visualizing Large-scale Data	Custom
[213]	Graph Theory	Inferring Malicious Network Events	CAIDA
[215]	Link Analysis - Parallel Coordinate Plots	Building a Network Traffic Visualization System	Custom
[222, 223]	Pattern Recognition - Image Processing	Detecting Traffic Anomalies	Custom
[221]	Hough Transform	Proposing a Technique to Detect Scanning Activities	Custom
[218, 219]	Game Engine	Enabling Collaborative Network Control	Custom
[220]	Game Engine - Greynet	Visualizing Network Data	L3DGEWorld - OpenArena
[224]	Parallel Coordinate Information Visualization	Detecting and Visualizing Network Threats	PCAV - CAIDA
[225]	Hilbert Curve Mapping	Facilitating the Analysis of Large-scale Events	CAIDA
[216, 217]	IDS	Visualizing Various Backscattered and Scanning Traffic	InetVis

Table 3.19: Visualization Research Papers - Summary

in the traffic features through simple patterns. Their technique was implemented and its efficiency was demonstrated by comparing it with another statistical analysis technique. A variety of network traffic anomalies were detected by analyzing traffic from /18 network address space. They also propose a tool for visualizing and exploring network traffic on all temporal and spatial scales. Their tool aims to help researchers inspect traffic with basic features [223].

Fukuda et al. [221] propose a technique to detect scanning activities in darknet traffic. They aim to estimate probing speed of change in terms of destination addresses, source ports and destination ports. Their method is based on an image processing technique applied to a two-dimensional image that represents unwanted traffic. They employ the progressive probabilistic Hough transform algorithm to detect edges in an image representing unwanted activities as lines. The authors apply their method on darknet traffic traces collected over a three-year period. They concluded that most of the scanning activities were characterized by intensive scans to a specific host. Furthermore, they found that few port scanning activities take place over a wide destination port space. Harrop and Armitage [218, 219] describe a system where a 3D game engine technology is used to enable collaborative network control. The proposed approach leverages simplistic interaction techniques by translating network events into visual activities. Their idea is to monitor a darknet network state that is represented in the 3D world by avatars spinning and jumping to visually alert network operators to a network anomaly. Subsequently, the operators can detect and shoot the alerting avatars to trigger a firewall access control list on a border router, preventing any further attacks. In a similar work, Parry [220] describe the L3DGEWorld project that is based on the OpenArena open source game engine platform. The approach aims to visualize network data based on the engine of a specific game. The approach describes the input interface to the L3DGEWorld server, which can be used to visualize and represent data in a real-time fashion. Moreover, the proposed approach also describes the output abstraction layer, through which data is connected from the virtual platform to the external daemon on the output interface.

Furthermore, several contributions attempt to visualize backscatter data from darknet. For instance, Choi et al. [224] build a model to detect and visualize network threats on parallel coordinates. This parallel coordinate attack visualization (PCAV) tool is able to detect zero-day attacks such as DDoS. PCAV operates based on several coordinates in a packet such as source and destination IPs, ports, and average packet length. Nine signatures were developed based on a hashing algorithm. Following the detection phase, network administrators must intuitively recognize and respond to the threat. This flow-based tool was proven to be efficient when applied to backscatter data. Furthermore, Irwin and Pilkington [225] develop a tool for facilitating the analysis of large-scale darknet traffic. In particular, the tool focuses on the analysis of data coming from different sources. The authors preserve the concept of nearness among numerical sequential IP address blocks using a Hilbert curve technique as a means of ordering dots within a visualization area. The authors also visualize the evaluation of worm spread algorithms. They further discussed the results and the importance of such tools to facilitate the analysis of big data. Riel and Irwin [216] propose InetVis, a visualization tool for darknet traffic. This tool plots TCP and UDP packets within a cube and ICMP packets within a flat plane. The authors adopt a time window to continue displaying an event after it has occurred. The researchers capture thousands of packets to test their tool. They observed numerous probing activities such as vertical and horizontal scans, step up scans (scan on the same port followed by stepping up the port range) and slow scans. Similarly, the authors in [217] demonstrate and compare InetVis with two open source NIDSs, Snort and BRO, where the advantages of the former are discussed. In this work, InetVis was re-implemented and enhanced. The authors argue that their tool is effective in visualizing various backscattered and scanning traffic while not suffering from high rates of false positives and negatives as do the other NIDSs.

It is noteworthy to mention that various tools exist on the Internet for darknet data visualization and analysis. The aim is typically to facilitate the analysis, the display, the collection and the presentation of the data. We list below tools from CAIDA [226] such as Cuttlefish for producing animated images that uncover the connection between the diurnal and geographical patters of data; GTrace for graphically trace-routing the destination; Geoplot for creating geographical images of data; LibSea for representing big directed graphs in memory and on disk; Mapnet for visualizing the infrastructure of multi-backbone providers; Otter for showing arbitrary communication information that can be presented as a group of nodes, connections or paths; Plankton for illustrating international cache topology; Plot-latlong for geographically mapping hosts; PlotPaths for displaying reverse and forward packets from one to one or one to many connections; and finally Walrus for representing large graphs in 3D.

3.3.1 Summary

In the last part of this darknet taxonomy, we have discussed several techniques and tools for darknet visualization. From what has been discussed in the that part of Section VI, we can conclude the following points:

- Several research works attempt to visualize darknet data by leveraging various techniques. The majority of these visualization techniques fall into two main areas, namely, generic-based and threat-based.

- Generic-based techniques aim at providing a graphical representation of usual darknet data (i.e., backscatter), whereas threat-based ones visualize darknet threats (i.e., DDoS).

- Generic-based techniques leverage mainly graph theory, whereas threat-based ones utilize mainly pattern recognition and image processing.

- Nevertheless, graph theory and game engines methods are used in both generic-based and threat-based techniques to model darknet network traffic.

- The majority (66.6%) of the visualization techniques are used to visualize threats on darknet.

- Although darknet data is similar to any network traffic, CAIDA research center is the primarily contributor to develop designated darknet visualization tools to depict large-scale events and threats.

- The visualization of darknet data is the smallest part of our darknet taxonomy.

3.4 Related Surveys

As previously discussed, a thin line distinguishes darknet from other trap-based monitoring systems such as IP gray space [48, 49], greynet [24], honeytokens [227] and darkports [228]. However, two main groups of surveys can be related to our work. The first group focused solely on a specific technology or threat whereas the second elaborated on trap-based monitoring systems.

First, various surveys tackled the detection techniques in network traffic such as NIDS [229], threats such as DDoS [230], botnet [231, 232] and worms [233], and malicious activities such as scanning [234]. Compared to our work, this group of research focused on a specific technology or a threat only whereas ours was more comprehensive. For instance, our survey included not only a study on DDoS threats, but also provided an overview on several darknet topics that can be leveraged to infer various insights from the Internet, including threats, events, techniques and tools.

Second, in regard to surveys that tackled trap-based monitoring systems, Zhang et al. [235] were among the first to classify honeypots in 2003. They highlighted data capture and data control in honeypots. Furthermore, they provided a classification of these traps based on security and application purposes. Furthermore, Seifert et al. [236] presented a taxonomy of honeypots. The authors described a classification of honeypots based on several schemes and were able to distinguish between seven types of honeypots (i.e., low and high interactive). In 2012, Bringer et al. [237] divided honeypot research into 5 major areas: types of honeypots, analysis of data, configuration, detection of sensors, and legal and ethical issues. The main difference between the works in [235–237] and ours is the scope of the survey. This group of works focused on honeypots, including active monitoring. Complementary, our work focused solely on passive monitoring of unused IP addresses. The only work that touched darknet research is [236] by discussing darknet and comparing it to other monitoring systems (low and high interactive honeypots). Our work is more comprehensive in regard to darknet study as it covers development, data analysis, and visualization.

Therefore, our survey is more close to the second group of contributions which tackled trap-based monitoring systems. Our survey complements the aforementioned related research works. Furthermore, the realistic analysis and investigation of real data provides more understanding and hands-on investigation experience on darknet data and threat analysis. We provided a guideline to develop, analyze and visualize real cyber insights by leveraging darknet data. The extracted darknet knowledge in our work can help in building a cyber intelligence platform for Internet monitoring. For more details on our survey, we refer the reader to [8].

After this broad study of darknet, in the next chapter, we start investigating real darknet data.

Chapter 4

Darknet Investigation

In this chapter, we initiate our darknet data investigation. In this context, we elaborate on profiling darknet data. Such information could generate indicators of cyber threat activity as well as providing an in-depth understanding of the nature of its traffic. Particularly, we analyze darknet packets distribution, its used transport, network and application layer protocols and pinpoint its resolved domain names. Furthermore, we identify its IP classes and destination ports as well as geographically locate its source countries. We further investigate darknet-triggered threats. The aim is to explore darknet embedded threats and categorize their severities. Finally, we contribute by exploring the inter-correlation of such threats, by applying association rule mining techniques, to build threat association rules. Specifically, we generate clusters of threats targeting a specific victim.

In this context, the aim of this chapter is to answer the following set of questions:

1. What is the nature of darknet traffic and its underlying content?

2. Who contributes to darknet traffic?

3. Are there any embedded darknet threats?

4. Can we show that such threats are correlated and hence provide their real world interpretation and impact?

To answer these questions, the work presented in this chapter contributes in the following three aspects:

- *Analysis accuracy:* The analyzed darknet data includes packet types that were omitted by other research works (i.e., ICMP in [111]). As such, the data set is rich which contributes to a better accuracy of the analysis.

- *Threat analysis:* By adopting an analysis methodology based on the use of network intrusion detection systems (NIDSs), our approach yields real world threats that are embedded in darknet traffic. Such results will be presented in Section 4.2.1.

- *Association rule mining approach:* By applying association rule mining and correlation techniques on the threat data, we investigate clusters of threats that co-occur. Such cyber threat intelligence proves that specific threats are correlated in addition to providing a better understating by interpreting the attack scenarios targeting specific network destinations.

4.1 Darknet Measurements

In order to better understand the nature of darknet data, we primarily provide an overview of darknet traffic and insights on large volumes of darknet traffic emanating from numerous organizations. Second, we discuss three case studies related to separate events, namely, probing, botnet and DRDoS activities. Our dataset is collected from several sources of real-life data such as CAIDA[1] and DShield[2].

[1] CAIDA Dataset: http://www.caida.org/data/

[2] DShield: https://www.dshield.org/

4.1.1 Inside Darknet

To understand the nature of darknet data, we provide an overview of its traffic. The dataset is pure darknet data captured during a five-year period from a single unused /8 network address block [2].

Count	TCP	UDP	ICMP
Packet	76.6%	19.9%	2.8%
Bytes	55.82%	40.82%	2.66%

Table 4.1: Protocols Distribution - Inspired by [2]

Table 4.1 lists the distribution of darknet transport and network layer protocols. It is shown that the majority of darknet traffic consists of TCP packets. Several facts can explain the TCP dominance. First, TCP provides various scanning techniques (i.e., SYN, Fragmentation, SYN-ACK) [238]. Second, generating TCP scanning is generally more feasible than UDP [239]. Finally, as noted in [108], well-known cyber attacks are specifically targeting TCP services.

Port	Service
445	microsoft-ds
139	NetBIOS
4662	eDonkey
80	HTTP
135	Endpoint Mapper

Table 4.2: Top TCP-based Services

We further list top application protocols found on darknet. Table 4.2 depicts the top 5 TCP-based services that have been observed based on [2]. The results demonstrate that the Microsoft Directory Service (microsoft-ds) is leading while the NetBIOS is ranked second. The former service is known to be abused by malware such as Conficker worm [176]. More information on the Conficker worm can be found next.

4.1.2 Case Studies

Base on real darknet data analysis, we provide three case studies on separate events, namely, Conficker worm in 2008 and 2009, Sality SIP scan botnet in 2011, and the largest DRDoS attack in 2014.

Case Study 1 - Conficker Worm in 2008 and 2009

In 2008, a new exploit targeted Windows services. Consequently, Microsoft announced a security update (MS08-067) to resolve the issue. The threat originated from a malicious TCP scanning behavior by a worm named Conficker [240]. The latter is a malware designed to exploit victim machines by exploiting TCP port 445 (Microsoft Directory Services). Conficker infected millions of computers in over 200 countries, which render it one of the largest known computer worms. In this case study, we show the outcome of the darknet analysis that inferred random scans generated by this worm. The dataset of the attack on the 20^{th} and 21^{th} of January 2009 is shown in Figure 4.1.

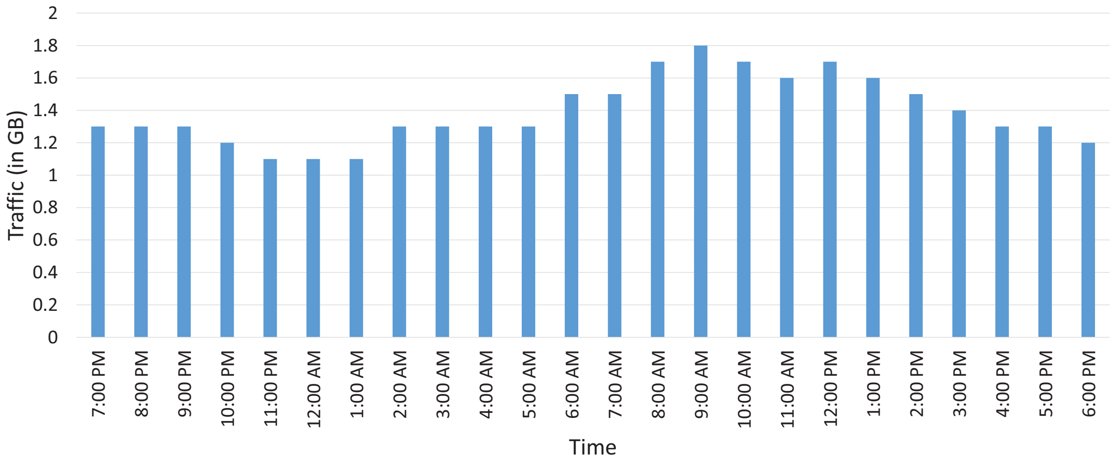

Figure 4.1: Conficker Worm in 2009 - Traffic Distribution (1 hour interval)

Several versions of Conficker (A and B) were involved in the attack. It is noteworthy to mention that the figures depict the peak at 2 pm in the analyzed 2009 dataset. However, based on the analysis done by other researchers, the attack also peaked at 2 pm during the 2008 dataset [240]. This could pinpoint the orchestration and automation of the machinery behind the attack, which is shown as a diurnal pattern in [240, 241].

Case Study 2 - Sality Botnet SIP Scan in 2011

In February 2011, the Sality botnet executed a /0 SIP scan through the whole IPv4 address space. This 12-day event involved 3 million unique IP addresses in one of the most coordinated cyber scanning campaigns ever. The botnet generated 20 million scans to 14.5 million addresses, which is almost 86.6% of the whole /8 monitors. This campaign targeted SIP services, which run on port 5060 and threatened the voice communications infrastructure. The darknet observation of this event is depicted in Figure 4.2. The campaign initiated in January and ended in February, 2011. The attack peaked at 21,000 hosts within a 5-minute interval. More on this attack can be found in [28].

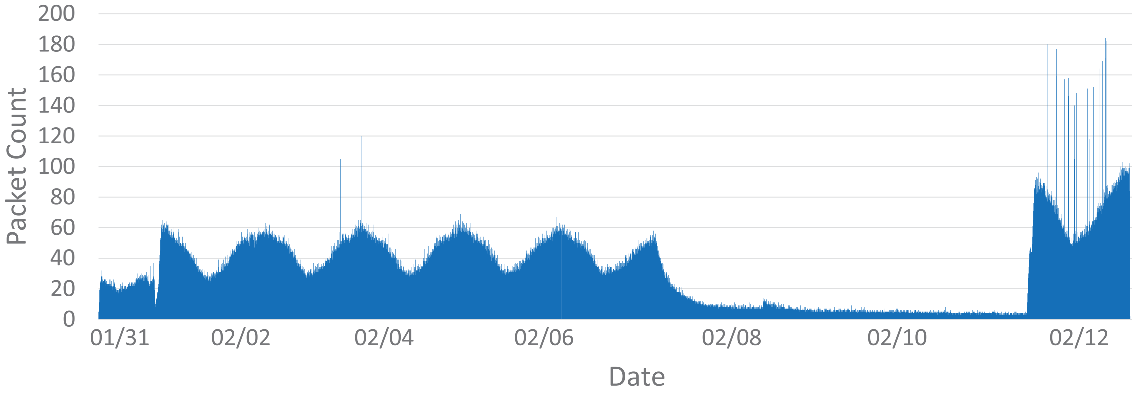

Figure 4.2: Sality Botnet SIP Scan in 2011 - Traffic Distribution (12 days)

Case Study 3 - The Largest DRDoS Attack in 2014

In 2013, a 300-Gbps DRDoS attack targeted Spamhaus [211]. In February 2014, the largest DRDoS attack in history, which peaked at 400 Gbps of bandwidth, hit the Internet infrastructure. We have depicted the latter attack through the DShield data in Figure 4.3. This image shows the source distribution of UDP-based packets on port 123-NTP (in yellow) with the corresponding generated reports (in blue). The graph depicts the increase in NTP packets and reports during the attack.

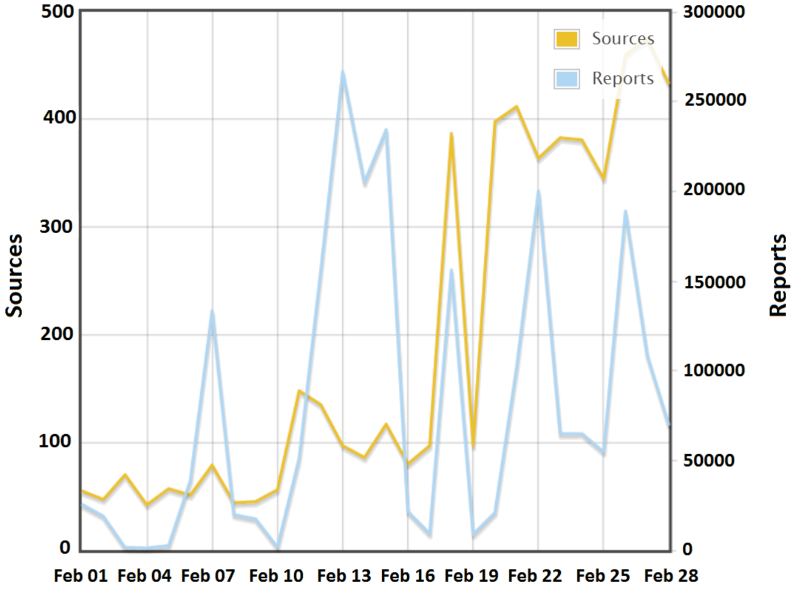

Figure 4.3: The Largest NTP-based DRDoS Attack in History

Typically, in an NTP amplification attack, the adversary generates a flood of spoofed UDP network packets. This large amount of traffic is sent to open Network Time Protocol servers, which operates at port number 123. This attack abuse the MONLIST service in NTP with an aim to send amplified traffic to the victim. More on NTP amplification DRDoS attacks in the context of darknet can be found in [242]. Similar to NTP amplification DRDoS attacks, DNS service can also be abused to generate amplification/DRDoS attacks. More on DNS amplification and DRDoS activities through darknet analysis can be found in [31, 243].

The aforementioned darknet measurements and case studies provide a basic understanding on what is darknet and how it is leveraged to generate cyber intelligence. Next, we start characterizing darknet, but this time using our own data, which is obtained from our trusted partner at Farsight Security.

4.2 Darknet Profiling

Similarly, we have performed darknet traffic profiling on our monitored sensors. To accomplish this task, we analyzed some darknet data collected in the period between September 16th, 2011 and May 9th, 2012. The analyzed data feeds are retrieved in real-time from a trusted third party framework[3]. The data consists of pure darknet traffic collected from many countries and monitor `/13` address blocks.

We initiated our analysis by differentiating darknet packets according to their types following the method in [2]:

- Scanning traffic; TCP SYN packets
- Backscattering traffic, which commonly refers to unsolicited traffic that is the result of responses to attacks with spoofed source IP address; TCP SYN+ACK, RST, RST+ACK, and ACK packets
- The remaining traffic packets are classified as misconfiguration

Scanning Traffic	Backscattering	Misconfiguration
68.02%	2.00%	29.98%

Table 4.3: Packets Distribution - Nature of Traffic

Table 4.3 depicts the outcome distribution. These results reveal that scanning or network probing constitutes the majority of darknet traffic. Note that, such traffic could be interpreted as an indication of port scanning and/or vulnerability probing. Such attacks, in general, are preliminary triggered before launching a targeted attack towards a specific system. We next aim to identify the major protocols that are used in darknet traffic. Table 4.4 provides the percentages of darknet transport and network layer protocols. It is observed that TCP plays the major role.

[3] Farsight Security: https://www.farsightsecurity.com/

TCP	UDP	ICMP	Others
91.9%	5.5%	2.9%	0.3%

Table 4.4: Protocols Distribution

Figure 4.4 corroborates this fact by plotting the protocols distribution in a day sample, which is the average of daily samples collected over a month's period. TCP dominance can be explained by two facts: First, the majority of scanning attacks use TCP and second, there exist known attacks that specifically target TCP ports as noted in [108]. TCP increase in Figure 4.4, especially after the 12^{th} hour, indicates that the darknet sensors record an increasing number of TCP packets after that period.

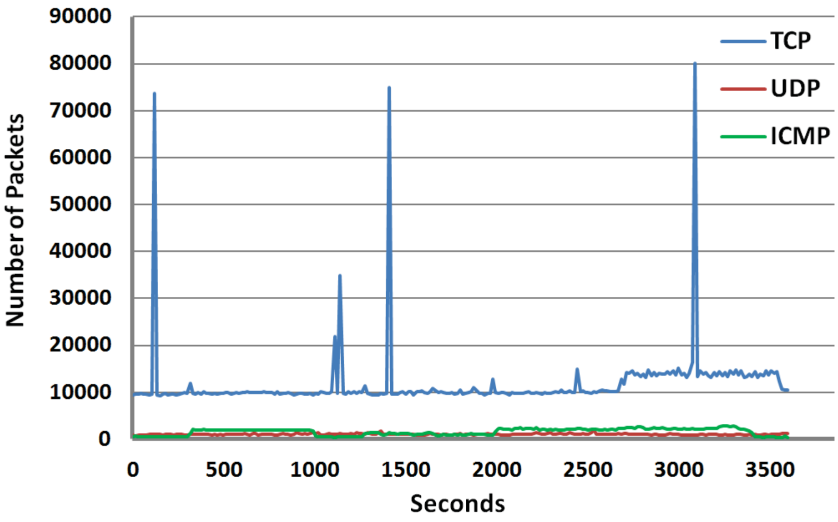

Figure 4.4: Darknet Network and Transport Layer Protocols

Such information pinpoints the need for a thorough temporal analysis and comparison of that phenomenon, which may uncover and explain the occurrence of certain attacks at specific time periods and their absence during other periods at any given day. Next, we profiled darknet application protocols. Figure 4.5 illustrates the top 16 application protocols that have been found. The results demonstrate that the Session Initiation Protocol (SIP) is leading while the Domain Name Service is ranked second and NetBIOS is ranked third. It is worthy to note that the SIP protocol is excessively used in DoS attacks, specifically against voice over IP (VoIP) servers [244], and thus its appearance as a top darknet application protocol is significant and may be alarming.

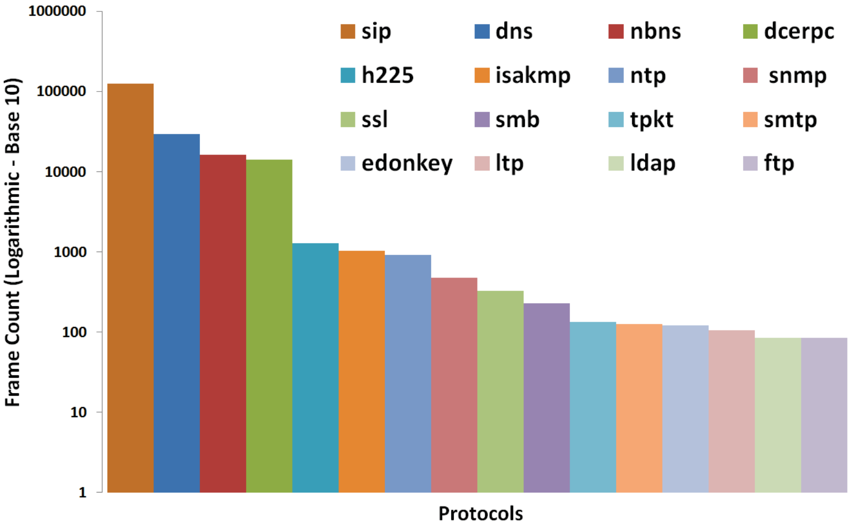

Figure 4.5: Darknet Application Layer Protocols

We further studied the source and destination distributions of IP classes in the darknet traffic. Table 4.5 depicts the results.

	Usage (%)	
Class	Source	Destination
A	62.529	0.017
B	18.529	7.138
C	18.942	92.845

Table 4.5: IP Class Distribution

It is revealed that the majority of source IPs belong to class ‘A’, whereas in the case of destination IPs, class ‘C’ plays the major role. Furthermore, Class ‘A’ proportion in the destination IPs is almost negligible, i.e., 0.017% whereas class ‘B’ contributes relatively more. It is substantial to mention that class ‘C’, being the most destined and smallest class, could be an indication that it is as well the most targeted class by cyber attacks and hence further investigation in it could yield relevant cyber intelligence. Moreover, we were interested in identifying the resolved domain names in darknet. After performing this task, we identified that the top-most darknet resolved domain belongs to a `.cc` Internet country code top-level domain for Cocos (Keeling) Islands. Note that this domain, according to the anti-phishing working group, constituted a significant 7.3% of all phishing attacks detected in 2010 [245]. Similar results could feed us, in general, with relevant information about unsolicited/malicious domains that could be used by attackers. Another analysis has been performed on the TCP and UDP ports that are used in the collected darknet traffic. Specifically, we aimed to pinpoint the destination ports. Such insights could reveal the targeted ports used in cyber attacks. Figures 4.6 and 4.7 illustrate such results.

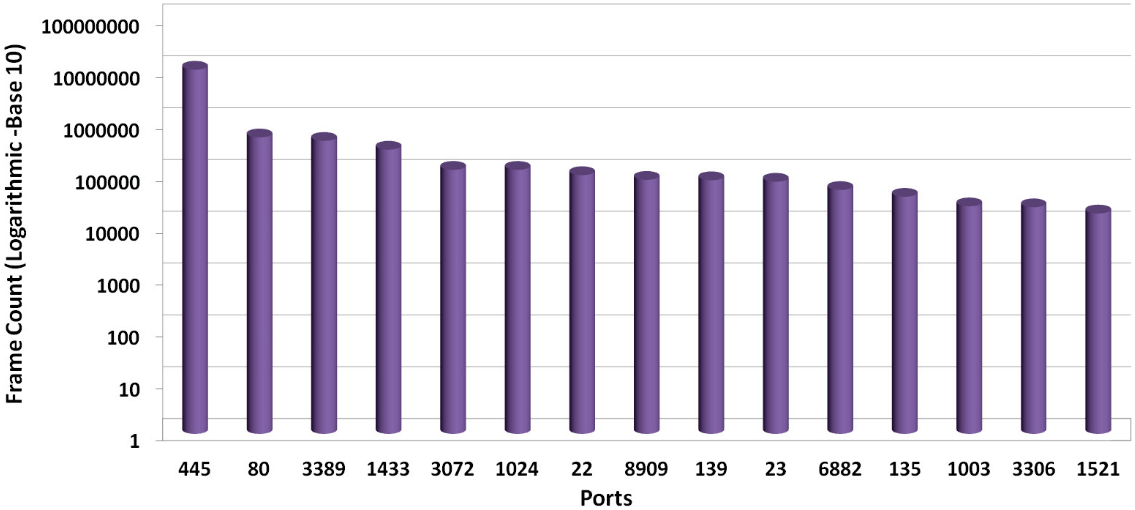

Figure 4.6: Darknet TCP Targeted Ports

The top three destination darknet TCP ports, namely, ports 445, 80, and 3389 are the Microsoft active directory service, the hypertext transfer protocol, and the Microsoft terminal server respectively. These service ports have previously suffered from security issues and vulnerabilities. A sample of the threats targeting such services are pinpointed in [246], [247] and [248] respectively. Hence, it is alarming that

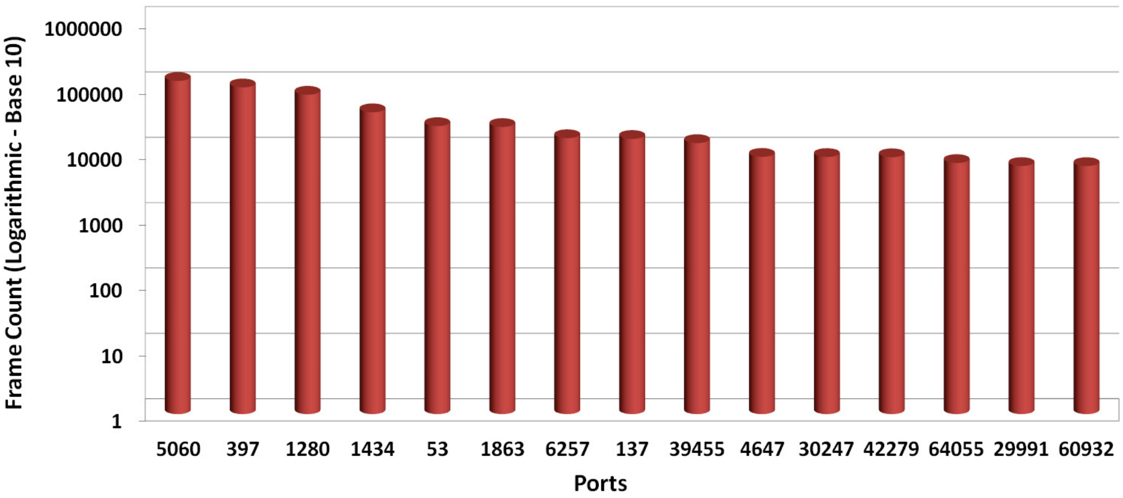

Figure 4.7: Darknet UDP Targeted Ports

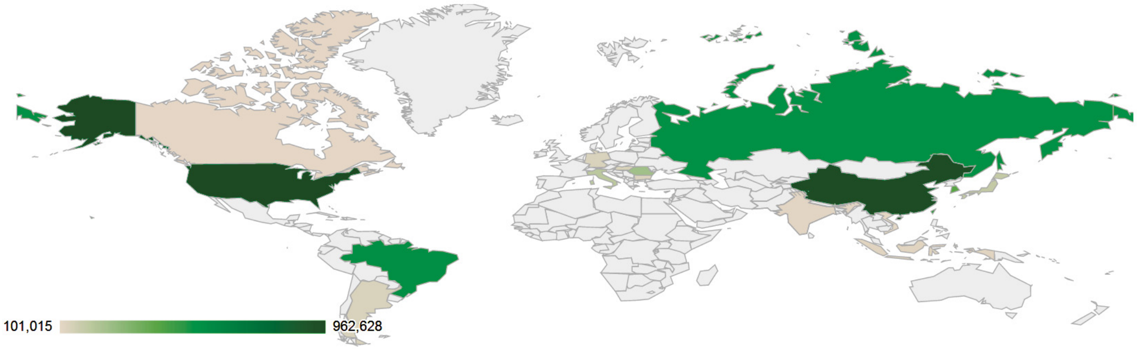

Figure 4.8: Darknet Sources - Heat Map

such ports appear as the top darknet destination TCP ports. On the other hand, the top three destination darknet UDP ports, namely, ports 5060, 397, 1280 are the SIP, the multi-protocol transport network (`mptn`) service, and the pictography protocol respectively. The SIP protocol, as mentioned previously, is a significant target of attack. This result further validates the integrity of our insights. Moreover, the `mptn` and the pictography services are known to suffer from denial of service attacks when a malformed request is destined to them. For the purpose of pinpointing the sources that contribute to the darknet traffic, we perform darknet geo-localization. Figure 4.8 depicts the heat map. According to our analysis, the source countries reached 196 countries where the majority of source IPs are located in USA. It is as well noticeable that Brazil, China, and Russia represent the major portion of source IPs compared to other countries. Note that, in Section 4.2.1, when we reveal the darknet threat analysis and geo-locate the sources behind those threats, the three aforementioned countries as well appear amongst the top contributed threat countries.

4.2.1 Threat Analysis

In this section, we extend our profiling task to uncover real world threats that are embedded in darknet traffic in addition to categorize their severities and geo-locate their sources. For that purpose, we executed threat-based severity analysis. To accomplish this task, Snort [41] and Bro [249], two open source NIDSs, combining the benefits of signature, protocol and anomaly-based inspection, were implemented and utilized. Part of their content signature detection, Snort and Bro implement the Boyer-Moore exact string matching detection algorithm in addition to a non-deterministic finite automata regular expression detection algorithm. To perform the threat analysis, we configured the NIDSs with rule sets from the Sourcefire Vulnerability Research Team and The Bro Network Security Monitor. Consequently, we fed the darknet data to the NIDSs. A partial outcome of this procedure is summarized in Table 4.6. The results reveal 30 distinct threats. According to the NIDSs, three threats are of high priority, two are of medium severity and the

Threat	Type	Priority
t_1	Buffer Overflow Exploit	High
t_2	Denial of Service	
t_3	VPN Attempt	
t_4	Traceroute Utilization	Medium
t_5	Service Port Discovery	
t_{6-30}	Scanning Attempts	Low

Table 4.6: Darknet Threats and Corresponding Severities

rest are of low priority. The first high priority threat (t_1) is in fact an attempt to possibly overflow a buffer. Specifically, a series of NOOP (no operation instructions) were found in the data stream. Typically, most buffer overflow exploits use NOOP commands to modify code operation [250]. Hence, this threat might indicate an attempt to use a buffer overflow exploit. Thus, a full compromise of a system is possible if the exploit is successful. Another high priority threat (t_2) is rendered as an attempt to cause a DoS. Particularly, a heap-based buffer overflow in Microsoft MSN Messenger [251] is found on Windows systems. This vulnerability allows user-assisted remote attackers to execute arbitrary code via unspecified vectors involving video conversation handling in Web Cam and video chat sessions. As a result, DoS and complete administrator access to a targeted system is possible. The last high priority threat (t_3) is in reality a detected virtual private network (VPN) remote attempt on a set of darknet addresses. Although, in general, VPN is not considered a threat, however an attempt to gain VPN access on a specific system can be alarming. On the other hand, threats t_4 and t_5, and according the NIDSs, are of medium severity. Threat (t_4) represents an attempt to use a traceroute software where an attacker can discover live hosts and routers on a target network in preparation for an attack. Moreover, (t_5) is a portmap `GETPORT` request to discover the port where the Remote Procedure Call (RPC) `statd` is listening. An attacker can query the port mapper to discover the port where statd runs. Consequently, this may be a precursor to accessing statd. The remaining of the incidents are mainly scanning attempts and are considered of low severities. Although their techniques may vary, their end goal is to either perform port scanning or vulnerability probing in preparation to a possible targeted attack. It is very significant to note, for the purpose of results integrity, that such scanning attempts, that constitute the majority of the threats, are in accordance with our darknet profiling results, specifically the packets distribution - nature of traffic percentages (68.02%) that was demonstrated in Table 4.3 in Section 4.2. For the purpose of accomplishing a high level attribution, we perform geo-location of the threat sources. Figure 4.9 depicts the heat map. Note that the threat count metric is of the order of thousands. The results reveal that Russia and China lead in terms of number of inferred threats.

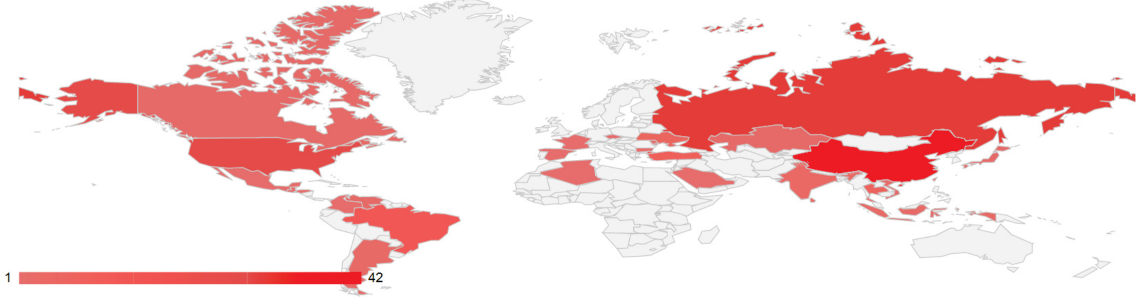

Figure 4.9: Threats Sources - Heat Map (in thousands)

4.3 Threats Correlation

There is a crucial need to further analyze the threats that have been previously detected and discussed. This section explores the inter-correlation of such threats, by applying association rule mining techniques, to build threat association rules. Such work demonstrates that specific darknet threats are in fact correlated or co-occur when targeting specific victims. Moreover, it provides insights about threat patterns and allows the interpretation of threat scenarios.

4.3.1 Approach

The goal of this approach is to investigate the interdependence and inter-correlation of inferred threats. Particularly, we aim to answer the following questions: Are there any threats targeting a specific victim that follow a certain pattern? Moreover, if some of the co-occurring threats appear in a darknet traffic, how confidently one can predict the existence of other threats? To investigate this, we employed the technique of frequent pattern mining (frequent item-set) and association rule mining [252]. Another outcome of this approach, besides the ones mentioned above, is the generation of threat association rules that could be used as an input to a classification model that is able to predict and hence mitigate future threat occurrences. Frequent pattern and association rule mining techniques have been proven to be very successful for identifying hidden patterns in DNA sequences, customer purchasing habits, text categorization, and many other applications of pattern recognition. The proposed threat correlation approach is a three-step process, namely, frequent pattern mining, association rule generation from each frequent threat-set, and rule analysis by applying various correlation techniques. Each of these steps is detailed below.

Frequent Pattern Mining

An item-set or a pattern is a group of two or more objects that appear together. An item-set is a *frequent* pattern if its members appear together for some minimum number of times. In the context of threat analysis, an item or an object is a threat and an item-set is the threat-set.

Time Intervals	Identified Threats
τ_1	$\{t_2, t_5, t_7, t_9\}$
τ_2	$\{t_2, t_5, t_7\}$
τ_3	$\{t_2, t_5\}$
τ_4	$\{t_1, t_5, t_7\}$
τ_5	$\{t_4, t_5, t_7\}$
τ_6	$\{t_3, t_6, t_8\}$
τ_7	$\{t_4, t_5, t_8\}$
τ_8	$\{t_3, t_6, t_8\}$
τ_9	$\{t_2, t_5, t_8\}$
τ_{10}	$\{t_1, t_5, t_7, t_8, t_9\}$

Table 4.7: Vectors of Darknet Threats

Table 4.7, which is used for illustration and explanation purposes, depicts 10 threat-sets, one threat-set per row. Let $T = \{t_1, \cdots, t_m\}$ denote the universe of all threats detected from the given darknet feeds F. Suppose a threat-set $T_i \subseteq T$ detected at a time interval τ_i represents a row or an instance in the threat table (Table 4.7). This latter shows ten threat-sets captured at time intervals $\{\tau_1, \cdots, \tau_{10}\}$. Let $T_i \subseteq T$ be a threat-set or a pattern in the threat table. A pattern that contains k threats is a $k-pattern$. For instance, $\tau_1 = \{t_2, t_5, t_7, t_9\}$ is a $4-pattern$. Similarly, the support of a pattern T_i is the percentage of all the instances T in the threat table containing T_i, denoted by *support*$(T_i|T)$. Note that the probability $P(t_a \cup t_b)$, where $t_a \cup t_b$ indicates that a pattern contains both t_a and t_b, is the union of itemsets t_a and t_b. The support is defined in equation 4.1:

$$\text{support}(t_a \Rightarrow t_b) = P(t_a \cup t_b) \tag{4.1}$$

A pattern T_i is a $frequent\ pattern$ if the support of T_i is greater than or equal to some user specified minimum support threshold, which is a real number in an interval of $[0, 1]$. Further explanation of these terms is given in Example 4.3.1.

Example 4.3.1 *Consider Table 4.7. Suppose the user-specified threshold* $min\_sup =$ 0.3*, which means that a pattern* $T_i = \{t_1, \cdots, t_k\}$ *is frequent if at least 3 out of the 10 rows contain all threat-items in* T_i*. For instance,* $\{t_2, t_5, t_7, t_9\}$ *is not a frequent pattern because it has support 1/10 = 0.1. Similarly,* $\{t_2, t_5\}$ *is a frequent 2-pattern because it has support 4/10 = 0.4 and contains two threats. Likewise,* $\{t_5, t_8\}$ *is a frequent 2-pattern with support* $3/10 = 0.3$.

There are various data mining algorithms for extracting frequent patterns, such as the Apriori [252], FP-growth [253], and ECLAT [254]. In this work, we employ the Apriori algorithm since it has been validated in several text mining studies [255]. Below, we provide an overview of the Apriori algorithm. Apriori is a level-wise iterative search algorithm that uses frequent k-patterns to explore the frequent

$(k+1)$-patterns. First, the set of frequent 1-pattern is found by scanning the threat table, accumulating the support count of each threat-set, and collecting the threat patterns containing T that also contains T_i with $support(T_i|T) \geq min\_sup$. The resulting frequent 1-patterns are then used to find frequent 2-patterns, which are then used to find frequent 3-patterns, and so on, until no more frequent k-patterns can be found. The generation of frequent $(k+1)$-pattern from frequent k-patterns is based on the following Apriori property.

Property 4.3.1 (Apriori property) *All nonempty subsets of a frequent pattern must be frequent.*

By definition, a pattern T_i' is not frequent if *support* $(T_i'|T) < min\_sup$. The above property implies that adding a threat t to a non-frequent pattern T_i' will not make it frequent. Thus, if a k-pattern T_i' is not frequent, then there is no need to generate $(k+1)$-pattern $T_i' \cup T$ because $T_i' \cup T$ is also not frequent. The following example shows how the Apriori algorithm exploits this property to efficiently extract all frequent patterns or threat-sets. For a formal description, we refer the reader to [252].

Example 4.3.2 *Consider Table 4.7 with* $min\_sup = 0.3$*. First, identify all frequent 1-patterns by scanning the threat table once to obtain the support of every threat-set. The items having support* ≥ 0.3 *are frequent 1-patterns, denoted by* $L_1 = \{\{t_2\}, \{t_5\}, \{t_7\}, \{t_8\}\}$*. Then, join* L_1 *with itself, i.e.,* $L_1 \bowtie L_1$*, to generate the candidate set* $C_2 = \{\{t_2, t_5\}, \{t_2, t_7\}, \{t_2, t_8\}, \{t_5, t_7\}, \{t_5, t_8\}, \{t_7, t_8\}\}$ *and scan the threat table once to obtain the support of every pattern in* C_2*. Identify the frequent 2-patterns, denoted by* $L_2 = \{\{t_2, t_5\},\{t_5, t_7\}, \{t_5, t_8\}\}$*. Similarly, perform* $L_2 \bowtie L_2$ *to generate* $C_3 = \{t_5, t_7, t_8\}$*. By scanning the threat table once, we found that* $\{t_5, t_7, t_8\}$ *is not frequent, i.e., 3-pattern* L_3 *is empty. The finding of each set of frequent* k*-patterns requires one full scan of the rows in Table 4.7.*

Association Rule Mining

The selected frequent patterns or frequent threat-sets are used to investigate the correlation and interdependence of the subsets of each frequent threat-set. This can be achieved by applying association rule mining techniques [256]. For this, all 1-patterns are deleted as they contain only one threat and thus can not be associated with any other threat. The 2-patterns threat-sets are used to extract single-dimensional association rules while the 3-patterns and higher patterns are used to construct multi-dimensional association rules. To construct an association rule of threats, we need to calculate the confidence for each frequent threat-set. The confidence is the percentage of threat-sets containing threat Y in addition to threat X with regard to the overall number of threat-sets containing X. Assume we have a threat-set $\{t_a, t_b\}$ for which the association rule would be $\{t_a\} \Rightarrow t_b$. Hence, the association rule has a confidence c in the threat table T, where P is the probability and c is the percentage of threat-sets in T containing t_a that also contains t_b.
This statement is mathematically expressed in Equation 4.2.

$$\text{confidence}(t_a \Rightarrow t_b) = P(t_b|t_a) = \frac{support\{t_a \cup t_b\}}{support\{t_a\}} \tag{4.2}$$

Having support-count of $(t_a \cup t_b)$ and t_a, we can calculate confidence$(t_a \Rightarrow t_b)$ using Equation 4.2. Once the frequent threat-sets are extracted, the related association rule of a frequent threat-set T_i can be constructed as follows:

- Generate all non-empty subsets of T_i
- For every non-empty subset S, construct a rule $(S \Rightarrow (T_i - S))$, provided that the $\frac{support(T_i)}{support(S)} \geq min\_conf$

Correlation Analysis

In order to investigate the interdependency of the threats, various correlation techniques including χ^2, *cosine* measure, and *lift* [256] can be used. In the current study, we use *lift*, which is based on probabilities and its results are interpretable by non-technical domain experts without the help of data mining experts. The correlation technique *lift* measures how many times more often threats t_a and t_b occur together than expected if they are statistically independent. The lift indicates whether the identified threat patterns are correlated together. It is mathematically expressed as follows:

$$\text{lift}(t_a, t_b) = \frac{P(t_a \cup t_b)}{P(t_a)P(t_b)} \tag{4.3}$$

If the value of Equation 4.3 is equal to 1 then threats t_a and t_b are independent and therefore have no correlation; otherwise they are either negatively correlated (i.e., *lift* < 1) or positively correlated (i.e., *lift* > 1).

4.4 Empirical Evaluation

Darknet Feed Providers	**Analyzed Address Blocks**	**Association Rules**	**Confidence**	**Lift**	**Count**
Destination Network 1	w1.x1.y1.z1/24	1.$\{t_7, t_8, t_9\} \Rightarrow t_{10}$ 2.$\{t_{10}, t_{14}, t_{13}\} \Rightarrow t_{11}$	0.63 0.56	3.64 7.06	282 306
Destination Network 2	w2.x2.y2.z2/24	3.$\{t_{10}, t_{15}, t_4\} \Rightarrow t_1$ 4.$\{t_{12}, t_{11}, t_{13}\} \Rightarrow t_{10}$	0.76 0.92	1.54 3.81	193 359
Destination Network 3	w3.x3.y3.z3/24	5.$\{t_{10}, t_7, t_8, t_9, t_{13}\} \Rightarrow t_4$ 6.$\{t_{10}, t_8, t_9, t_{13}\} \Rightarrow t_{12}$	0.55 0.26	10.75 3.68	218 348
Destination Network 4	w4.x4.y4.z4/24	7.$\{t_7, t_8, t_9\} \Rightarrow t_{10}$ 8.$\{t_4, t_8, t_9\} \Rightarrow t_{10}$	0.43 0.98	4.12 6.6	113 102
Destination Network 5	w5.x5.y5.z5/24	9.$\{t_{10}, t_7, t_8, t_9, t_{13}\} \Rightarrow t_{11}$ 10.$\{t_7, t_8, t_9, t_{11}, t_{13}\} \Rightarrow t_{10}$	0.41 0.82	3.56 3.65	260 131

Table 4.8: Darknet Threat Patterns

We used Weka [257] to run the Apriori algorithm. In summary, the Apriori algorithm takes the threat table in ARFF file type as input along with the user-defined parameters including minimum support *min_sup* and confidence c, and generates association rules. To assess our approach, we experimented with different threats that were detected and mentioned in Table 4.6. The experimental results are achieved by employing sequential rule mining techniques for correlating same set of threats. Consequently, the generated rules can be used to build an associative classification model for predicting the occurrences of specific threats in real-time darknet traffic. In general, the threat rules generated by the Apriori algorithm, provided the threshold is kept low, is usually very large. However, we can tune and filter the results to bring the rules to a manageable level by applying the following steps:

- Choosing a suitable value for the minimum support based on the occurrence count of the targeted threat. Note that the choice of selecting a minimum support threshold is inversely proportional to the number of generated threat-sets.

- Taking into consideration the size of the association rules by specifying the number of items per threat-set as input to the algorithm.

- Removing threats, prior to the analysis, that do not contribute in information gain (i.e., a threat that is absent during the analyzed period).

In the current work, we selected a portion of darknet providers network blocks as the target of attacks. Specifically, we restricted the target of the attacks to five `/24` network blocks. Table 4.8 represents our frequent pattern and association rule mining results. For confidentiality and privacy matters, we anonymized some sensitive information. This table discloses the analyzed IP blocks, their corresponding identified threat patterns or association rules, coupled with their lift, confidence and number of occurrences per day. The latter metric is an indication that the identified threat pattern is valid since it frequently occurs per unit of time (a day in our current analysis). Up to this point, we have demonstrated that certain darknet threats are in fact correlated or co-occur when targeting specific network destinations. For example, consider association rule 1 in Table 4.8. This rule discloses that if we detect threats $\{t_7, t_8, t_9\}$ in some order in the live darknet data stream, then with 63% confidence, we can as well expect to predict that threat t_{10} will follow or occur. Note that these threats are correlated since the value of the *lift* is > 1. In the sequel, we attempt to provide an interpretation to the identified threat patterns. Please refer to the numbered association rules in Table 4.8 as a reference to the below interpretations. It is worthy to note that such interpretations are solely derived from the threat patterns and the NIDSs threat descriptions. Hence, we aimed to provide the most logical and best fit scenario considering the threat association rules. We believe that one interesting outcome of this work is the ability to provide insights about threat patterns and interpret real world threat scenarios. Future work in this area could provide more elaborative interpretations.

The first association rule discloses the following information. A Unix host, running FreeBSD, attempts to fingerprint a target Voice over IP (VoIP) Session Initiation Protocol (SIP) server on port 5060. By fingerprinting, the attacker hopes to retrieve server identification information such as operating system and installed services. Finally, the attacker leverages the attack by sending an enormous number of malformed ICMP packets directed towards the SIP server. The latter can be interpreted as a denial of service attempt. The second association rule reveals the subsequent information. An exploited Windows host first attempts to ping a target to check if it is alive. To retrieve more information, the adversary initiates various traceroute commands. Moreover, the attacker attempts to connect to a certain undisclosed port. However, he is faced with an "unable to connect" error message. The latter effort can be explained by an attempt to gain system access. The third association rule can be interpreted as the following. A typical attacker first performs port and host scanning to identify security vulnerabilities and possible ways to get system access. Sequentially, he can trigger various traceroute commands to retrieve more information on how to reach his target. Finally, he will attempt to execute a high priority threat (a buffer overflow exploit) to gain elevated privilege on the victim's system. The fourth association rule presents a scanning attack targeting IP version 6. Specifically, it discloses that an attacker first attempts to fingerprint a server running IPv6. After receiving a request timed out reply, he launches a traceroute command to further explore his target's path. Finally, he extends his attack by sending a series of ICMP packets. The latter can be interpreted as a denial of service attempt against the IPv6 server. The fifth association rule discloses the following information. A Unix host, running FreeBSD as an operating system, attempts to fingerprint a target server on TCP port 80. By fingerprinting, the attacker hopes to retrieve the server's (possibly the web server's) identification information such as operating system and installed services. This can be a prelude to discovering vulnerabilities and sequentially instrumenting a targeted attack. His scanning request is made from a Flowpoint 2200 DSL router. However, the reply is a message indicating that such port is unreachable. In an attempt to gather more information about the target, the attacker consequently launches various traceroute commands. The sixth association rule can be interpreted as the following. An attacker aims to target a Microsoft server running as a domain controller. The server, running Windows 2000 Server, has the Microsoft directory services installed and running. The attacker first tries pinging the server to see if it is operational. After receiving a positive confirmation, he elevates his attack by tracing the path to reach the server. Finally, he leverages his attack by sending an enormous number of malformed ICMP packets directed towards the domain controller. The seventh association rule is a series of scanning attempts on UDP port 53, a port normally dedicated for the domain name service (DNS). A host running Windows 9x generated a significant number of ICMP echo requests directed towards the server. In an attempt to gather more information about the target, the attacker consequently launches traceroute commands. The eighth association rule unveils the following information. An attacker launches various traceroute commands from a Unix host. He leverages his scanning attempts by sequentially targeting TCP port 3389, the Windows Remote Desktop Protocol (RDP). This event is alarming since it can be interpreted as an attempt to gain system access especially if the mentioned service is vulnerable or if its authentication is inadequately configured. The ninth and tenth association rules are syntactically different, however contextually, they can be interpreted similarly. They disclose that an exploited host is generating enormous malformed ICMP packets towards a certain target. This is an indication of an attempt to launch a denial of service attack against the target victims.

4.5 Related Work

Several studies explored darknet traffic analysis. We can classify these proposals into two main categories. The first category is based on designing, implementing and managing darknet platforms, while the second focuses on the analysis of darknet traffic feeds.

In the following, we describe some of the projects in the area of darknet monitoring systems. In [25], the author presented Honeyd as a framework for the deployment of honeypots using virtual machines. This project runs on unallocated addresses within various operating systems. Such environments provide numerous services which aid in detecting and mitigating worms, preventing spam distribution and alerting about suspicious attacks. Another project is the network telescope which was proposed in [75] to monitor cyber incidents through the dark address space. Moreover, the Internet Motion Sensor (IMS) system, a distributed system, described in [62], reports the network behavior originating from different monitored IP blocks. Furthermore, Yegneswaran et al. [52] developed Internet Sink (iSink) to monitor unused IP address space. The iSink approach was conceived to address the scalability issue that is related to large address spaces. It incorporates passive detection and monitor sensors as well as honeynet components.

In the other category, namely darknet analysis, the research in [108] elaborated on a detailed analysis of the darknet data. Their active and passive analyses assessed darknet samples from different networks and over a long time period. Another study [2] has reviewed the last mentioned work to render the state of this Internet background radiation at that current year. The authors observed significant changes and pinpointed several factors that are behind these measures. Moreover, Fukuda et al. [258] studied correlations among darknet traffic for estimating their behaviors through small address blocks by analyzing a specific type of traffic packets (i.e., TCP SYN). There are other research proposals that investigated threats triggered through darknet such as in [164] where the authors were able to study the Slammer worm. Moreover, denial of service (DoS) attacks were as well addressed in [30] by analyzing the replies of DoS attacks from spoofed sources in darknet feeds. Other studies such as [259] elaborated on scanning events, misconfiguration and other suspicious activities.

4.6 Summary

In this chapter, we investigated darknet by performing darknet characterization and threat profiling. We interpreted the output of this step by providing insights as indicators for cyber threat activity. Particularly, the results can be summarized in the following: Scanning traffic constitutes the majority of darknet traffic; TCP leads the darknet protocol distribution; SIP contributes as the major darknet application layer protocol; IP Class ‘C’ is the most destined class of darknet traffic; TCP port 445, pertaining to Microsoft active directory service, is the most targeted port. We presented and discussed darknet-triggered threats. Distinctively, we highlighted various threats as well as their severities and elaborated on their nature and consequences. This analysis step revealed three high severity threats, namely, denial of service attempts, buffer overflow exploits and unsolicited VPN access. Furthermore, we explored the inter-correlation of such threats, by applying association rule mining techniques, to build threat association rules. Such work demonstrated that, in fact, certain darknet threats are correlated when targeting specific network destinations. Moreover, it provided insights about threat patterns and allowed the interpretation of threat scenarios. Among the identified threat clusters was one leading to a high priority buffer overflow exploit. For future work, we intend to provide more cyber threat insights and build a classification model from the threat association rules to experiment its predictability features with near real time darknet traffic.

In the next chapter, we will be focusing on the prediction of DDoS events as well as DDoS cyber campaigns.

Chapter 5

Prediction Model for DDoS Activities

After providing some analytics on darknet data and threats, in this chapter, we generate intelligence in regards to DDoS activities. In fact, we propose a DDoS forecasting model to provide significant insights to organizations, security operators and emergency response teams during and after a targeted DDoS attack. Specifically, the work strives to predict, within minutes, the attacks' impact features, namely, intensity/rate (packets/sec) and size (estimated number of used compromised machines/bots). The goal is to understand the future short term trend of the ongoing DDoS attack in terms of those features and thus provide the capability to recognize the current as well as future similar situations and hence appropriately respond to the threat. Our analysis employs real darknet data to explore the feasibility of applying the forecasting model on targeted DDoS attacks and subsequently evaluate the accuracy of the predictions. To achieve these tasks, our proposed approach leverages a number of time series fluctuation analysis and forecasting methods. The extracted inferences from various DDoS case studies exhibit promising accuracy with very low error rate. Further, our model could lead to a better understanding of the scale and speed of DDoS attacks and should generate inferences that could be adopted for immediate response and hence mitigation as well as accumulated for the purpose of long-term large-scale DDoS analysis.

When an organization is subject to a DDoS attack, it becomes essential for its IT security staff to answer the following questions:

- What are the characteristics of a DDoS attack?
- During a DDoS attack, what is the future short term trend (i.e., within minutes) of the attack in terms of intensity/rate and size?
- After a DDoS attack, in terms of those impact features, what was the impact of the attack and what are the lessons learned?
- Is it an isolated DDoS attempt or a campaign of attacks against multiple victims?

The answers to these questions greatly influence the actions and the resources that the organization will choose to employ in responding to such malicious activity for the current incident as well as for future occurrences. For instance, the organization would often care more about high impact DDoS attacks, those that can cause serious disruption of a service in a relatively timely manner. If the latter is observed, the organization can immediately respond and tweak its mitigation methods to gauge the threat (i.e., forward the attack flow to a specific number of servers and/or dynamically assign specific firewall rules to handle the flood). This can reduce the response time and cost for an organization. Note that, low-rate DDoS attacks could be as worrisome as high impact ones, which might indicate that the DDoS attack is attempting to evade detection and at the same time exhaust the victim with long-lived flows [260]. Moreover, having knowledge about the short term (i.e., in terms of minutes) predicted impact features of the ongoing DDoS would provide various inferences to the organization and aid in answering the following questions: Will the DDoS increase or decrease in its intensity? Will the attack rate fluctuates? Will the botnet targeting that specific organization increase? Will the DDoS cease after few minutes or will it persist for a longer period of time? Further, the insights extracted from such an analysis on numerous DDoS occurrences targeting that organization could generate attack patterns that could be useful for future mitigation. For example, if the organization observes 5 distinct DDoS attacks in different time periods where they all possess similar rates, size and prediction parameters, then it can be inferred that the attacks originate from a single (or at least similar) botnet and hence point to a suspicious DDoS campaign. At a larger scale, such analysis aims at providing computer emergency response teams and observers of cyber events with DDoS trends, taking into consideration the botnet size and the bots geographic distribution, the victims geographic location, types of DDoS and bots that could be inferred from rate and intensity distributions, as well as future short term DDoS trends targeting various global-scale organizational sites. The latter outcome could be used for immediate response and alerting for mitigation purposes as well as for long term large-scale DDoS analysis.

In this context, this chapter's contributions are as follows:

- Proposing and adopting a systematic approach for inferring DDoS activities, testing for predictability of DDoS traffic and applying prediction models.

- Leveraging various time series analysis and forecasting methods, including, detrended fluctuation analysis, moving average, weighted moving average, exponential smoothing and linear regression.

- Characterizing and predicting DDoS attacks' impact features, namely, intensity/rate and size.

- Proposing a clustering approach to infer similarities among attack traces for DDoS campaign detection.

- Evaluating the proposed approach using real DDoS traffic.

5.1 Attack Prediction

This section presents and discusses various aspects of our forecasting model. The main components of our proposed approach is depicted in Figure 5.1.

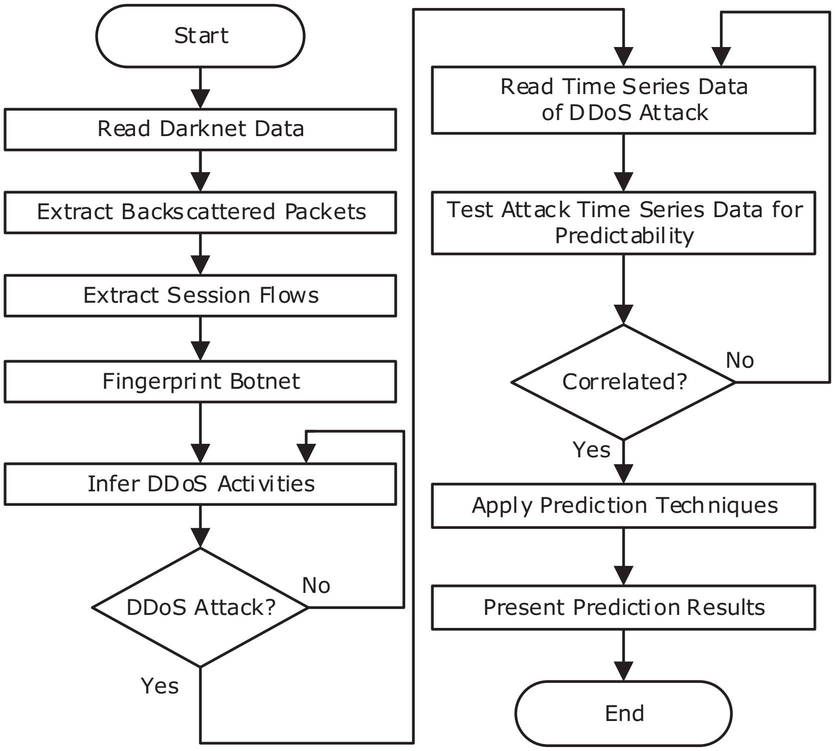
Start
Read Darknet Data
Extract Backscattered Packets
Extract Session Flows
Fingerprint Botnet
Infer DDoS Activities
DDoS Attack?
No
Yes
Read Time Series Data of DDoS Attack
Test Attack Time Series Data for Predictability
Correlated?
No
Yes
Apply Prediction Techniques
Present Prediction Results
End

Figure 5.1: Flow Chart of the Proposed Approach

In short, the approach is rendered by extracting backscattered data and session flows from darknet traffic. Subsequently, DDoS activities are inferred and consequently tested for predictability. Finally, prediction techniques are applied on DDoS traffic, when applicable. The proposed approach is detailed next.

5.1.1 Extracting Backscattered Packets

In order to extract backscattered packets, we adopt the technique from [2] that relies on flags in packet headers, such as TCP SYN+ACK, RST, RST+ACK, and ACK. However, this technique might cause misconfiguration as well as scanning probes (i.e., SYN/ACK Scan) to co-occur within the backscattered packets. In order to filter out the misconfiguration, we use a simple metric that records the average number of sources per destination darknet address. This metric should be significantly larger for misconfiguration than scanning traffic [261]. The scanning packets are filtered out in the next step.

5.1.2 Extracting Session Flows

In order to filter out the scanning activities, we split the connections into separate session flows, each of which consists of a unique source and destination IP/port pair. The rationale for this is that DDoS attempts possess a much greater number of packets sent to one destination (i.e., flood) whereas portsweeps scanners have one or few attempts towards one destination (i.e., probe).

5.1.3 Inferring DDoS Activities

We next aim to confirm that all the extracted sessions in fact reflect real DDoS attempts. To accomplish this, we employ a modified version of the DDoS detection parameters from [262] to label a session as a single DoS attack. Algorithm 1 lists our detection mechanism.

We decided to leverage the latter work since it is directly applicable to our work, which is based on a flow-based approach and leverages backscattered traffic to infer DoS attacks from darknet traffic. We proceed by merging all the previously extracted sessions that have the same source IP (i.e., victim) to extract the DDoS attack.

Algorithm 1 DDoS Detection Engine

```
In the algorithm:
Each flow $f$ contains packet count ($pkt\_cnt$) and rate ($rate$)
$Tw$: Time Window
$p\_th$: Packet Threshold
$r\_th$: Rate Threshold
$Tn$: Time of packet number $n$ in a flow
$pkt$: Packet

**Input:** A set of darknet flows $F$ where each $f$ in $F$ is composed of a pair of
<source IP, destination IP> leveraging a series of consecutive packets that share
the same source IP address.
**Output:** DDoS attack flows

for each $f$ in $F$ do
    $attack\_flag = 0$
    $pkt\_cnt = 0$
    $T1$ = pkt_gettime(1)
    $Tf = T1 + Tw$
    while $pkt$ in $f$ do
        $Tn$= pkt_gettime()
        if $Tn < Tf$ then
            pkt_cnt++
        end if
    end while
    $rate = \frac{pkt\_cnt}{Tw}$
    if $pkt\_cnt >$ p_th & $rate > r\_th$ then
        attack_flag = 1
    end if
end for
```

5.1.4 Testing for Predictability

A time series is a sequence of data values that are measured at successive points in time and spaced at uniform time intervals [263]. In order to predict DoS features, we aim to test if the time series of DDoS flows are first correlated. Otherwise, our prediction model would be irrelevant. In order to accomplish this, we statistically test for predictability in such time series using the Detrended Fluctuation Analysis (DFA) technique. DFA was first proposed in [264] and has since been used in many research areas to study signals correlation. The DFA technique is summarized next.

The DFA method of characterizing a non-stationary time series is based on the root mean square analysis of a random walk. DFA is advantageous in comparison with other methods such as spectral analysis [265] and Hurst analysis [266] since it permits the detection of long range correlations embedded in a seemingly non-stationary time series. It avoids as well the spurious detection of apparent long-range correlations that are an artifact of non-stationarity. Another advantage of DFA is that it produces results that are independent of the effect of the trend [267]. Last but not least, this technique is applicable to darknet traffic [111].

Given a traffic time series, the following steps need to be applied to implement DFA:

- Integrate the time series. The time series of length N is integrated by applying

  $$y(k) = \sum_{i=1}^{k} (B(i) - B_{ave}) \tag{5.1}$$

  where $B(i)$ is the i^{th} interval and B_{ave} is the average interval.

- Divide the time series into “boxes” (i.e., bin size) of length n.

- In each box, perform a least-squares polynomial fit of order p. The y coordinate of the straight line segments is denoted by $y_n(k)$.

- In each box, detrend the integrated time series, $y(k)$, by subtracting the local trend, $y_n(k)$. The root-mean-square fluctuation of this integrated and detrended time series is calculated by

$$F(n) = \sqrt{\frac{1}{N}\sum_{k=1}^{N}(y(k) - y_n(k))^2} \tag{5.2}$$

- Repeat this procedure for different box sizes (i.e., time scales) n

The output of the DFA procedure is a relationship $F(n)$, the average fluctuation as a function of box size, and the box size n. Typically, $F(n)$ will increase with box size n. A linear relationship on a log-log graph indicates the presence of scaling; statistical self-affinity expressed as $F(n) \sim n^{\alpha}$. Under such conditions, the fluctuations can be characterized by a scaling exponent α, which is the slope of the line relating $logF(n)$ to $log(n)$. The scaling exponent α can take the following values, disclosing the "correlation status" of the traffic time series:

- $\alpha < 0.5$: anti-correlated

- $\alpha \approx 0.5$: uncorrelated or white noise

- $\alpha > 0.5$: correlated

- $\alpha \approx 1$: $1/f$-noise or pink noise

- $\alpha > 1$: non-stationary, random walk like, unbounded

- $\alpha \approx 1.5$: Brownian noise

In our work, if the application of DFA on the DDoS traffic time series outputs a "correlated" status, then we assert that it is predictable; else, we extract another DDoS flow and re-test it for predictability.

5.1.5 Predicting DDoS Attacks

Finally, to perform the predictions, we apply different types of forecasting techniques, namely, moving average, weighted moving average, exponential smoothing and linear regression. We have selected to leverage these techniques instead of other complex well-known models such as ARIMA and GARCH [268] since the latter require long-term (weekly, monthly, yearly, etc.) seasonal time series data, which is not true in our case that deals with short-term DDoS traffic. The selected methods are briefed next.

Moving Average (MA)

The single parameter of the model is estimated as the average of the previous x data points at time t in the time series. The MA is given by:

$$\widehat{x}_{t+1} = \frac{1}{k} * (x_t + x_{t-1} + ... + x_{t-k-1}) \tag{5.3}$$

where k is the smoothing window or period. Note that the forecast in this technique should not begin until the specified previous data are available.

Weighted Moving Average (WMA)

This technique is based on a numeric value known as the weight. In general, a WMA is more responsive to change in the time series data than a simple MA. The computation of the WMA estimated temporal average is given by [269]:

$$\widehat{x}_{t+1} = \frac{w_{t-k}x_{t-k} + ... + w_t x_t}{h} \tag{5.4}$$

where k is the chosen window size and h is the sum of the temporal weight, $h = w_{t-k} + ... + w_t$. In general, to obtain better results, the highest weight is given to the most recent periods.

Exponential Smoothing (ES)

This technique calculates the parameter of the estimated prediction value b as the weighted average of the last observation and the last estimate. The estimated value is given by:

$$\widehat{x}_{t+1} = \alpha x_t + (1-\alpha)\widehat{x}_t \tag{5.5}$$

where α is the smoothing factor and has a value between [0,1].

Linear Regression (LR)

This technique performs statistical analysis that assesses the association between two variables. This method is used to pinpoint the relationship among these variables. A simple LR is given by:

$$LR(y) = a + bx \tag{5.6}$$

where x and y are the variables, b is the slope of the regression line, a is the intercept point of the regression line and the y-axis.

Two main elements characterize this model, namely, the slope and the intercept, given by:

$$Slope(b) = \frac{N\sum XY - \sum X \sum Y}{N\sum X^2 - (\sum X)^2} \tag{5.7}$$

$$Intercept(a) = \frac{\sum Y - b\sum X}{N} \tag{5.8}$$

where N is the number of values or elements, X is the first score and Y is the second score. The slope describes the incline or grade of the line whereas the intercept is the point where the graph of a function intersects with the y-axis of the coordinate scheme.

Finally, to evaluate the performance of the prediction methods, we compute the absolute prediction error. The equation of the absolute prediction error is given by:

$$r(t) = \frac{|\widehat{X}_i(t) - X_i(t)|}{X_i(t)} \tag{5.9}$$

This error metric is defined as the absolute difference of the predicted value from the actual value divided by the actual value. The latter is a de-facto metric when computing the performance of a prediction model [270, 271].

Note that in our prediction, for the MA and the WMA algorithms, we run a solver [272] to automatically obtain the weight values that produces a relatively better prediction results. Furthermore, we adopt a time window that is equivalent to three data points in the time series. We believe this provides a good estimate for such models as also demonstrated in [273]. Future work would extend such analysis by experimenting with different time window sizes. Furthermore, as far as the ES algorithm is concerned, we again run a solver [272] to automatically choose the best value of α that optimizes the prediction error rate. We refer interested readers to [270, 274] for more details on the above mentioned prediction techniques.

5.1.6 Empirical Evaluation

We abide and closely follow the steps of our proposed approach that were discussed in Section 5.1 to present three real case studies targeting three different servers. The case studies respectively consist of TCP SYN flooding targeting an HTTP (web) server, TCP SYN flooding targeting a Domain Name System (DNS) and an ICMP (ping) flooding. The three case studies are summarized in Table 5.1.

The table shows the analyzed duration of the attack (in seconds), the attack's intensity in terms of number of generated packets, its average rate (packets/sec), its DFA value and its size in terms of number of used compromised machines/bots. In

Case Study	Analyzed Attack Duration (second)	Intensity (packet)	Rate (pps)	DFA Value	Size of Spoofed IPs
TCP SYN Flooding (HTTP)	3194	1799228	563.31	0.91	24
TCP SYN Flooding (DNS)	3550	29016	8.17	0.93	206
ICMP Flooding	3599	3577	1.00	0.67	1

Table 5.1: Summary of the Analyzed DDoS Case Studies

regards to our dataset, we leverage the same source of darknet data from our trusted third party. In terms of DFA computation, we utilize the DFA MATLAB code found in [275] and used 1ms as the bin size. Further, when applying the forecasting techniques, for the purpose of error calculation, we use two thirds (66.66%) of the DDoS traffic time series for training and one third (33.33%) for testing. It is also noteworthy to mention that when performing the prediction analysis, we chose a time series with bin size equal to one minute. We argue that such a choice is rational and should provide enough resources (i.e., time) to the organization under attack to act upon the observed values. The case studies are elaborated next.

TCP SYN Flooding on an HTTP Server

This case study refers to a DDoS TCP SYN flooding targeting an HTTP web server. From Table 5.1, we notice that this attack lasted 53 minutes, generated around 1.8 million TCP SYN packets, with an average of 560 packets per second from 24 unique spoofed IPs (i.e., bots). The value of the rate of the attack demonstrates the severity of this DDoS attack. Moreover, Figures 5.2 and 5.3 demonstrates the application of the forecasting techniques.

Note that, we attempt to predict this DDoS since its corresponding DFA result was shown to be "correlated" with a value equals to 0.91 as stated in Section 5.1.4). Figure 5.2 illustrates the attack's intensity distribution with its corresponding forecasting techniques. It is shown that the attack peaks with around 175 thousand

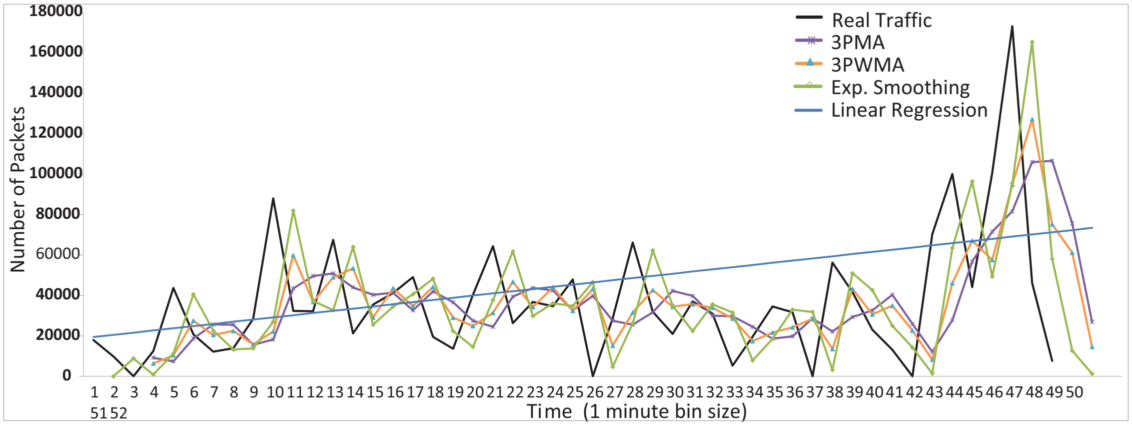

Figure 5.2: TCP SYN Flooding on an HTTP Server - Intensity Prediction

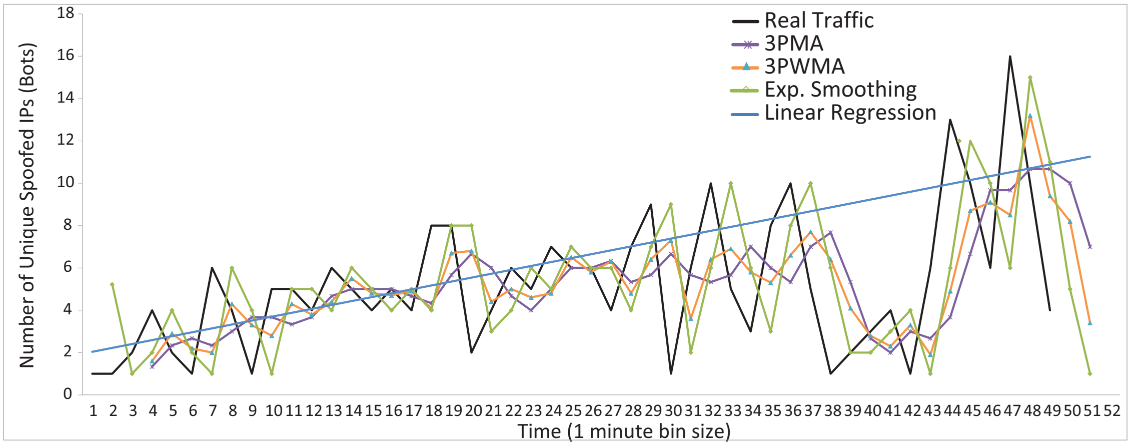

Figure 5.3: TCP SYN Flooding on an HTTP Server - Size Prediction

packets at the 46th minute. The predicted values (within the future 3 minutes) of such distribution reveal that the attack will decrease in intensity and fluctuates between 9000 and 3500 packets. On the other hand, Figure 5.3 illustrates the attack's size in terms of number of used spoofed IPs. It is shown that the number of spoofed IPs peak to 16 in the 48th minute. Similar to the intensity, it is shown from the prediction techniques that the size will as well decrease, hinting that the DDoS might soon diminish in size. The absolute prediction error of the forecasting techniques for this DDoS case study is summarized in Table 5.2.

We can notice that several techniques for both impact features recorded low error rates. Further, the exponential smoothing algorithm was best in predicting

	Prediction Techniques			
	MA	WMA	ES	LR
Intensity	0.57	0.39	0.19	0.86
Size	0.70	0.53	1.34	0.22

Table 5.2: HTTP-based TCP SYN Flooding - Absolute Prediction Error (%)

the intensity while the linear regression was best in predicting the size of the attack. This case study allows the organization whose web server is under a targeted DDoS to gain insight in terms of the current and future short term trend of the ongoing attack in terms of the defined attack impact features. Moreover, assuming that the organization modified its mitigation methods before predicting the future impact distributions, we reveal that such modifications are effective.

TCP SYN Flooding on a DNS Server

This case study refers to a DDoS TCP SYN flooding targeting a DNS server. From Table 5.1, we notice that this attack lasted 59 minutes, generated around 29 thousand TCP SYN packets, with an average of 8 packets per second from 206 unique spoofed IPs (i.e., bots). Although the size of this DDoS attack is larger than the first case study, however, its intensity in terms of the generated packets and hence rate is significantly lower.

Figures 5.4 and 5.5 depict the characterization in addition to demonstrating the application of the forecasting techniques. We also predicted this DDoS attack since its corresponding DFA result was shown to be “correlated” with a value equals to 0.93. Figure 5.4 illustrates the attack’s intensity and prediction distributions. It is shown that the attack peaks around 1600 packets at the 19$^{\text{th}}$ minute. The predicted values of such distribution shows insights of increase in the attacks intensity. On the other hand, Figure 5.5 reveals the attack’s size in terms of number of used compromised machines/bots. It is shown that the number of spoofed IPs peaks to

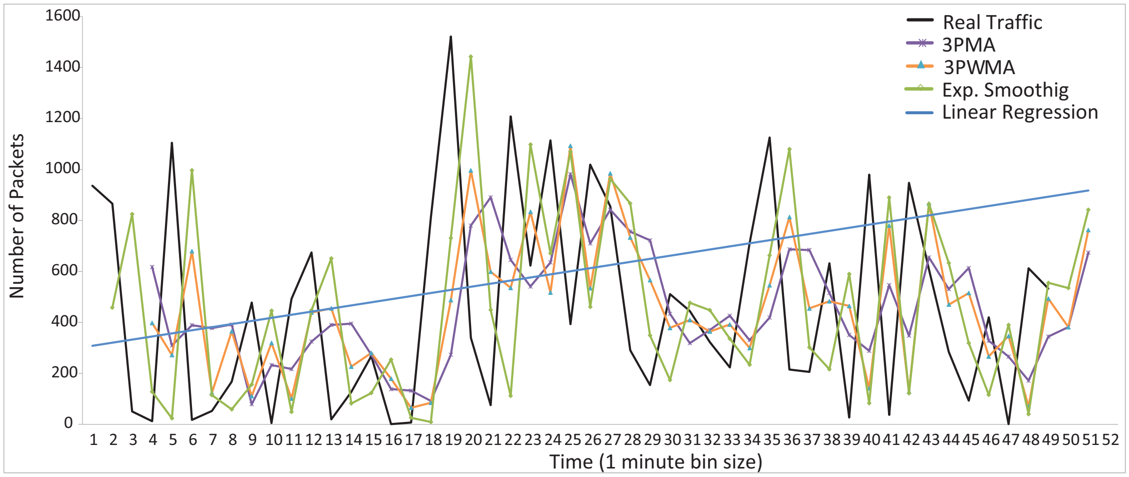

Figure 5.4: TCP SYN Flooding on a DNS Server - Intensity Prediction

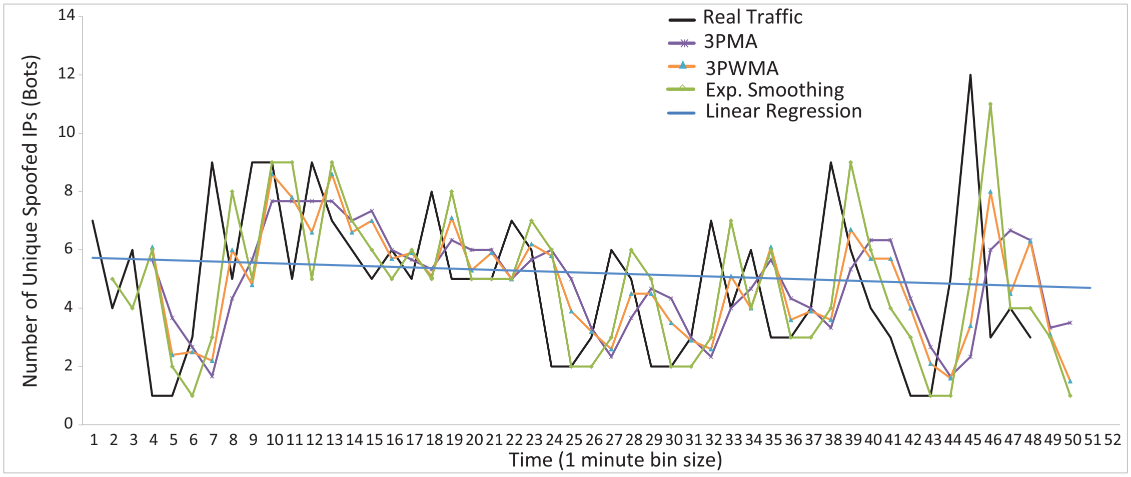

Figure 5.5: TCP SYN Flooding on a DNS Server - Size Prediction

12 in the 45th minute. Furthermore, it is shown from the prediction models that the attack size will either stay constant or slightly decrease.

The absolute prediction error of the forecasting techniques for this DDoS case study is summarized in Table 5.3.

We notice that the linear regression poorly performs with regards to this case study. Moreover, the exponential smoothing algorithm was best in predicting both the intensity and the size. This case study allows the organization whose DNS server is under a DDoS attack to be alerted that the attack's intensity might increase. This

	Prediction Techniques			
	MA	WMA	ES	LR
Intensity	12.46	5.24	2.75	35.71
Size	0.51	0.37	0.16	0.72

Table 5.3: DNS-based TCP SYN Flooding - Absolute Prediction Error (%)

provides the organization the capability to comprehend the situation and hence adaptively respond to the threat.

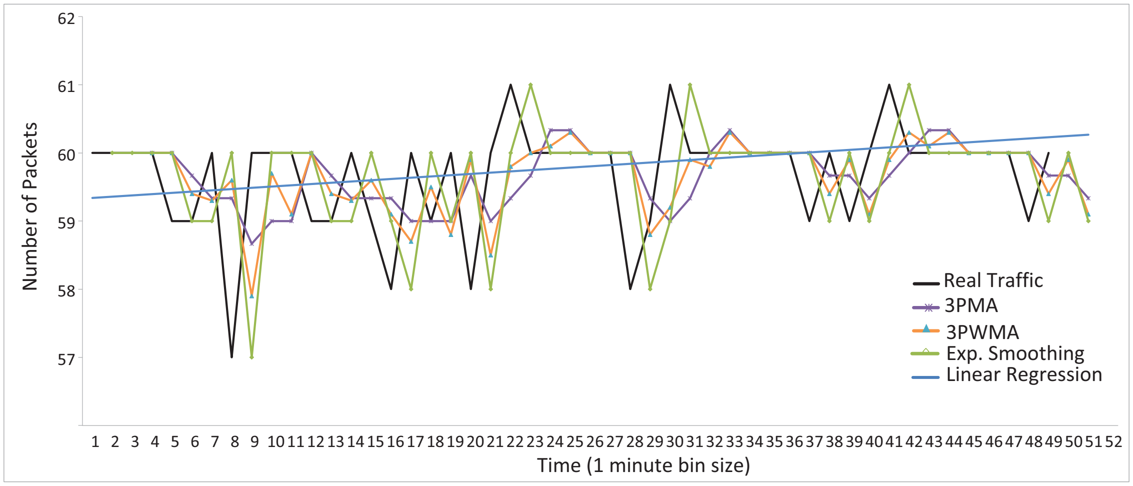

Figure 5.6: ICMP (ping) Flooding - Intensity Prediction

ICMP (ping) Flooding

This case study refers to a DoS ICMP (ping) flooding targeting a server. The major difference between this attack and the former case studies is that this attack is generated from only one machine (i.e., not distributed) and it could be attempting to evade detection by using a relatively low attack rate. Further, its DFA result shows signs of strong correlation (the DFA scaling exponent $\alpha = 0.67$) in its attack signal.

This is confirmed in Figure 5.6 where the intensity distribution fluctuates around 60 packets. From the prediction techniques, we can observe that the attack's

	Prediction Techniques			
	MA	WMA	ES	LR
Intensity	0.13	0.13	0.12	0.13

Table 5.4: ICMP (ping) Flooding - Absolute Prediction Error (%)

intensity will continue to be close to 60 packets or slightly increase. The summary of the result is shown in Table 5.4. Moreover, the attack's correlation and intensity features allow the organization whose server is under this type of DoS attack to infer that the attack is relatively of low impact and non-distributed and hence current mitigation methods will be sufficient.

5.2 Predicting Campaigns Targeting Multi-victims

In the previous sections, we elaborated on the components of the systematic approach for inferring DDoS activities targeting a unique organization, testing for predictability of such DDoS traffic and subsequently applying the prediction methods. In this section, we extend the model by proposing a clustering approach to infer DDoS campaigns that target multiple victims. The aim is to predict DDoS campaigns. Moreover, this permits the fingerprinting of the nature of such campaigns. For example, it could be identified that a specific DDoS campaign is specialized in targeting financial institutions while another campaign is focused on targeting various information communication technology infrastructures. Further, such clustering approach allows the elaboration on the actual scope of the DDoS campaign to provide cyber security situational awareness; how large is the campaign and what is its employed rates, when attacking the various victims. Additionally, the proposed approach could be leveraged to predict the campaign's features in terms of rate and number of involved machines.

5.2.1 Clustering of DDoS Campaigns

In this section, our approach employs the following statistical-based mechanism. First, backscattered sessions are extracted as previously discussed in Section 5.1. Second, the notion of fuzzy hashing [276] between the different sessions is applied. Fuzzy hashing is advantageous in comparison with typical hashing as it can provide a percentage of similarity between two traffic samples rather than producing a null value if the samples are different. This popular technique is derived from the digital forensics research field and is typically applied on files or images [276, 277]. Our approach explores the capabilities of this technique on backscattered DDoS traffic. We select the sessions that demonstrate at least 20% similarity. We concur that this threshold is a reasonable starting point and aids in reducing false negatives. Third, from those sessions, we employ two statistical tests, namely, the Euclidean and the Kolmogorov-Smirnov tests [278] to measure the distance between the latter selected sessions. We select those sessions that minimize the statistical distance and overlap after executing both tests. The rationale of the latter approach stems from the need to cluster the sessions belonging to multiple victims that share similar traffic behavior while minimizing the false positives by confirming such similarity using both tests. Note that, we hereafter refer to the use of the previous two techniques as the fusion technique. The outcome of the proposed approach are clustered diverse victims that are inferred to be the target of the same DDoS campaign.

5.2.2 Empirical Evaluation

In this section, we present the empirical evaluation results. We employ the DDoS campaign clustering model as discussed in the previous section to demonstrate how multiple victims could be modeled as being the target of the same campaign.

TCP SYN Flooding on Multiple HTTP Servers

To demonstrate the effectiveness of the approach, we experiment with a one day sample retrieved from our darknet data set. We extract 680 backscattered DDoS sessions and apply fuzzy hashing between the sessions, by leveraging deeptoad[1], a fuzzy hashing implementation. The outcome of this operation is depicted in Figure 5.7, where the victims are represented by round circles while directed arrows illustrate how the various victims were shown to be statistically close to other targeted victims. It is important to note that we anonymize the real identity of the victims due to sensitivity and legal reasons. Subsequently, the Euclidean and the Kolmogorov-Smirnov tests are executed to exactly pinpoint and cluster the victims that demonstrate significant traffic similarity. Figure 5.8 shows such result while Table 5.5 summarizes the outcome of the proposed DDoS campaign clustering approach. From Figure 5.8, one can notice the formation of root nodes, advocating that the approach is successful in clustering various victims that are the target of the same DDoS campaign.

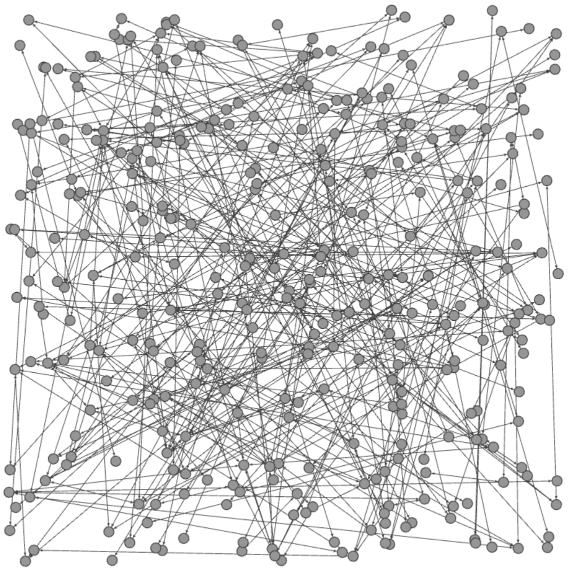

Figure 5.7: Clustered Victims Through Fuzzy Hashing

[1] https://code.google.com/p/deeptoad/

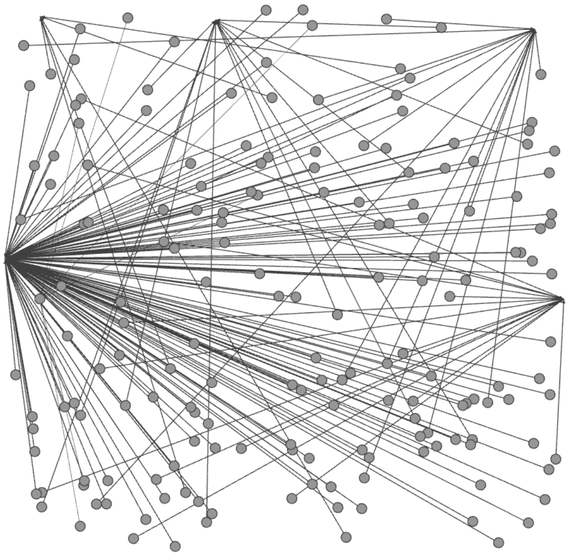

Figure 5.8: Clustered Victims Through the Fusion Technique

Technique	Unique Campaign Count	Campaign of 2 Victim Machines	Campaign of 3 Victim Machines	Campaign of 4 Victim Machines	Campaign of 5 Victim Machines	Campaign of 6 Victim Machines	Campaign of 125 Victim Machines
Euclidean	16	6	2	3	3	1	1
KS	16	6	2	3	2	2	1
Fusion	13	6	1	2	2	1	1

Table 5.5: Summary of the DDoS Campaign Clustering Approach

In general, the approach yielded, for one day data set, 13 unique campaigns where each campaign clusters a number of victims ranging from 2 to 125 targets. Recall that the fusion technique resembles the execution and overlap of the Euclidean and the Kolmogorov-Smirnov statistical tests.

We proceed by attempting to predict the impact features, namely, intensity and size, of one of the previously inferred DDoS campaigns. We select the last campaign of Table 5.5 since it targeted the most victims.

This case study refers to a campaign of DDoS TCP SYN flooding targeting various HTTP servers related to 16 victim organizations. From Table 5.6, we notice that this campaign lasted almost one day and generated around 650 thousand TCP SYN packets, with an average of 7 packets per second from 92296 unique spoofed IPs

Case Study	Victim	Analyzed Attack Duration (second)	Intensity (packet)	Average Rate (pps)	DFA Value	Size of Spoofed IPs
TCP SYN Flooding (HTTP)	125	85322	649299	7.61	0.81	92296

Table 5.6: Summary of the Analyzed DDoS Campaign Case Study

(i.e., bots). Further, Figures 5.9 and 5.10 depict the characterization and demonstrate the application of the forecasting techniques. We also predicted this DDoS attack since its corresponding DFA result was shown to be "correlated" with a value of 0.81. Figure 5.9 illustrates the attack's intensity and prediction distributions. It is shown that the attack peaks around 8000 packets at the 47th minute. The predicted values of such distribution shows insights of decrease in the attacks intensity. On the other hand, Figure 5.10 reveals the attack's size in terms of number of used compromised machines/bots. It is shown that the number of spoofed IPs peaks to 3100 in the 10th minute. Furthermore, it is shown from the prediction models that the attack size will stay constant for some time and then decreases. The absolute prediction error of the forecasting techniques for this DDoS campaign case study is summarized in Table 5.7.

Notice that the linear regression poorly performs with regards to this case study. Moreover, the exponential smoothing algorithm was best in predicting both the intensity and the size.

	Prediction Techniques			
	MA	WMA	ES	LR
Intensity	1.27	1.51	0.09	2.16
Size	1.26	1.11	0.09	2.14

Table 5.7: TCP SYN Flooding on Multiple HTTP Servers - Prediction Error (%)

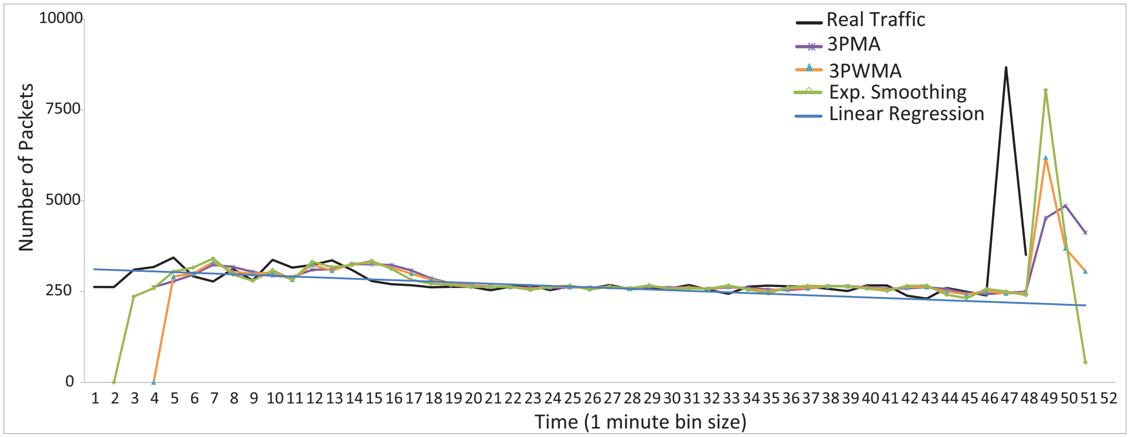

Figure 5.9: TCP SYN Flooding on Multiple HTTP Servers - Intensity Prediction

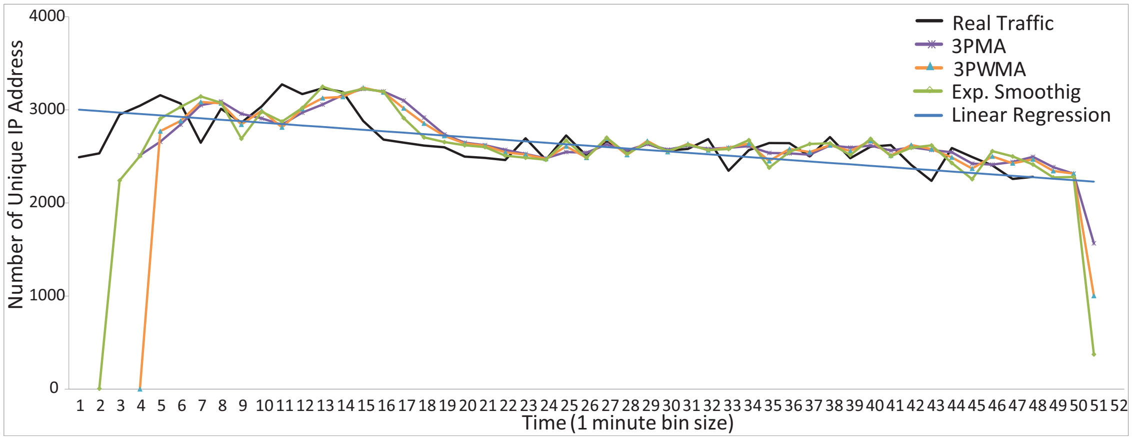

Figure 5.10: TCP SYN Flooding on Multiple HTTP Servers - Size Prediction

It should be noted that the generated inferences from the above case studies aim to better understand the scale and rate of DDoS attacks that could be adopted by organizations for immediate response and hence mitigation as well as accumulated by security operators, emergency response teams and observers of large-scale Internet DDoS events for the purpose of long term large-scale DDoS analysis, clustering and correlation.

5.3 Related Work

In this section, we provide a review of some relevant literature work in the area of threat prediction. In [279], the authors propose a method for threat prediction based on security events using a security monitoring system. Their approach consists of methods to collect and pre-treat security monitoring events, extract threads and sessions, create attack scenarios through correlation analysis, predict intrusions and express the analytical results. The authors evaluate the effectiveness of their prediction model by leveraging real security monitoring events. Dagon et al. [179] adopt a model to accurately predict botnet population growth. The authors use diurnal shaping functions to capture regional variations in online vulnerable populations. They state that since response times for malware outbreaks is measured in hours, the ability to predict short-term propagation dynamics permit resource allocation in a more effective and a suitable manner. The authors use empirical data from botnets collected at a sinkhole to evaluate their analytical model. Moreover, Fachkha et al. [142] present and discuss various darknet-triggered threats and their corresponding severity level. Furthermore, they explore the inter-correlation of such threats, by applying association rule mining techniques, to build threat association rules. Their work demonstrate that in fact certain darknet threats are correlated when targeting specific network destinations. Moreover, it provides insights about threat patterns and allows the building of a classification model for prediction purposes. In another work, Qibo et al. [280] propose an approach to detect and predict DoS SYN flooding attacks using non-parametric cumulative sum algorithm along with an ARIMA model. Instead of managing all real-time ongoing traffic on the network, the approach only monitors SYN packets to predict the attack in the near future. To perform the prediction, the authors propose the auto-regressive integrated moving average model. The authors also run some simulations to validate the effectiveness of the approach. In [281], the authors propose a forecasting mechanism called FORE (FOrecasting using REgression analysis) through a real-time analysis of randomness in network traffic. According to the authors, FORE can respond against unknown worms 1.8 times faster than other detection mechanisms. Evaluation results using real malware traffic demonstrate the efficiency of the proposed mechanism, including its ability to predict worm behaviors starting from 0.03% infection rate.

Most of the above discussed related work assumes that the threat traffic that needs to be predicted is in fact predictable. We argue that such assumption, without essential validation, might result in erroneous forecasting results, regardless of which forecasting approach has been employed. In contrary, in our work, we first statistically test for predictability before attempting to forecast. Additionally, we state that our work in terms of DDoS impact features characterization and prediction is distinctive since the leveraged DDoS inference algorithm is highly accurate and established [262] and does not depend solely on SYN packets. Moreover, our work has wide-scope benefits for security operators, security response teams as well as specific organizations for the short term as well as for the long term large-scale DDoS analysis. Moreover, our proposed approach is designed to effectively work on near real time data. Last but not least, for empirical evaluation purposes, we utilize a significant amount of real network traffic.

5.4 Summary

In Chapter 5, we primarily proposed an approach that is rendered by a DDoS inference and forecasting model. The aim was to provide the organization under attack the capability to comprehend the situation and hence adaptively respond to the threat. Second, the work proposed a DDoS campaign clustering approach that captures the similarity between backscattered sessions. The goal was to cluster various victims that are targeted by the same DDoS campaign. We characterized and predicted, within minutes, the attacks' impact features, namely, intensity/rate (packets/sec) and size (number of used compromised machines/bots). Our proposed approaches leveraged real darknet data to infer DDoS activities, test for predictability of DDoS traffic and apply prediction techniques, when applicable. Empirical evaluations presented several attack case studies to demonstrate possible extracted insights and inferences. For future work, we intend to experiment with more complex forecasting methods that can operate on probability or graph theory and long-term bases as well as implementing our proposed approach in a real-time fashion.

In the next chapter, we attempt to tackle the problem of fingerprinting amplification attacks.

Chapter 6

Analysis of Reflection (DRDoS) Attacks

In this chapter, we describe the design and implementation of a novel approach to infer reflection attacks through darknet. In order to facilitate the understanding of our approach, we primarily provide some basic concepts related to the mechanism of reflection DDoS attacks, and inferred darknet queries.

DRDoS Attacks: DNS Scenario

Amplification is a well known practice of a DDoS attack, in which malicious users abuse open amplifiers to bombard a victim with reply traffic [282]. The amplification technique consists of an invader directing queries to an amplifier having the source IP spoofed to be the victim's address. Subsequently, all server responses will be sent to the targeted victim. Amplification DRDoS attacks can abuse several services [32]. For instance, in a DNS scenario, malicious users will request domains that cover a large zone to increase the amplification factor. In this context, in order to have a high impact on the victim, the attackers use DNS requests of type `ANY` to return all possible known information to the victim, and hence increase the amplification of the attack. Moreover, in order to increase the size of the attack with little effort, attackers use botnets (i.e., campaigns) [283] to synchronize an army of bots and order them to send requests. Based on such concepts, Figure 6.1 depicts a basic DNS amplification attack with recursive DNS. In the first two steps, the attacker uses a botnet to generate spoofed DNS lookup requests to the Internet. In steps 3 to 7, the internal and external DNS servers collaborate in order to provide an answer to the requester. Finally, in steps 8 and 9, the amplified replies congest the victim's computer and network resources with a large flood of traffic.

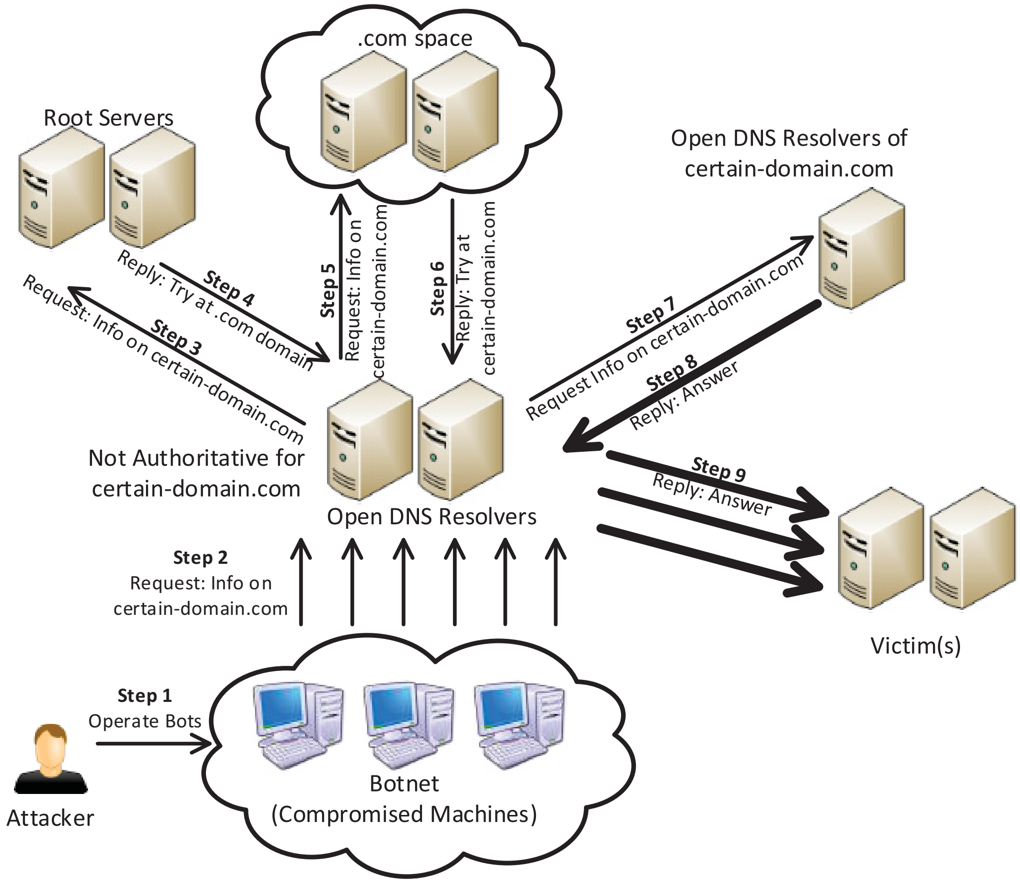

Figure 6.1: DNS-based DRDoS Scenario

Queries Found on Darknet

On darknet, we can observe a significant number of queries that could be sent by the following sources:

- *Attacker Spoofing the Victim's IP:* In this case, the attacker sends spoofed queries on the Internet address space using the victim's IP address. All replies from the open resolvers will bounce back towards the victim.

- *Compromised Victim:* In this case, the attacker uses the victim's machine to send queries. The attacker might use several techniques to control the victim's machine, including malware infection and/or vulnerability exploitation. This scenario does not involve spoofed queries.
- *Scanner:* In this scenario, the attacker scans the Internet to infer the locations of open amplifiers. This task requires collecting information from the reply packets and hence, a non-spoofed address is used by the scanners.
- *Others:* Other hosts may include firewalls to reduce the impact of the attack or misconfigured devices, etc.

In our work, we assert that high speed queries [282] will be sent from an attacker spoofing the victim's IP and/or compromised victim but not from a scanner. In other words, scanners might send queries to the Internet but with a low-speed rate to avoid receiving the amplified flood of replies. It is noteworthy to mention that our investigation in the next section includes DNS amplification analysis only. However, our approach identifies various attack types.

6.1 Inferring Internet Reflection Activities

After providing a background information on some reflection attacks found on darknet, we elaborate in this section on our novel approach to infer and characterize Internet-scale DNS DRDoS attacks by leveraging the darknet space. Complementary to the pioneer work on inferring DDoS activities using darknet [262], this work shows that we can extract DDoS activities without relying on backscattered analysis. The aim of this work is to extract cyber security intelligence related to DRDoS activities such as intensity, rate and geographic location in addition to various network-layer and flow-based insights. To achieve this task, the proposed approach exploits certain DDoS parameters to detect the attacks, and the expectation maximization and k-means clustering techniques to identify campaigns of DRDoS attacks. We empirically evaluate the proposed approach using 1.44 TB of real darknet data collected from a `/13` address space during a recent period of several months. Our analysis reveals that the approach was successful in inferring significant DNS amplification DRDoS activities, including the recent prominent attack that targeted one of the largest anti-spam organizations [211]. Moreover, the analysis disclosed the mechanism of such DNS amplification attacks. Further, the results uncover high-speed and stealthy attempts that were never previously documented. The extracted insights from various validated DNS DRDoS case studies lead to a better understanding of the nature and scale of this threat and can generate inferences that could contribute in detecting, preventing, assessing, mitigating and even attributing DRDoS activities.

In this context, we tackle the following questions:

1. How to infer large-scale DNS-based DRDoS activities?

2. What are the characteristics of DNS amplification DRDoS attacks?

3. What inferences can we extract from analyzing DNS DRDoS traces?

Answering those questions would aid computer security response teams, law enforcement agencies and governments to build a darknet-based central infrastructure to scrutinize DNS-based amplification traffic in order to contribute in understanding, detecting, preventing, assessing, mitigating and even attributing DRDoS attacks.

In this work, we frame our contributions as follows:

- Proposing a systematic flow-based approach for inferring DNS amplification DDoS activities by leveraging DNS queries to darknet.

- Characterizing the inferred DDoS threats during several months period.
- Applying clustering and similarity algorithms in an attempt to identify campaigns of DNS reflection DDoS attacks.

Next, we elaborate on our proposed approach.

6.1.1 Proposed Approach

This section presents our proposed approach that aims at generating darknet flows and inferring DNS-based DRDoS activities by leveraging darknet data. The approach exploits the idea of analyzing DNS queries that target the darknet that were originally intended by the attacker to reach Internet open DNS resolvers [31, 32]. The approach takes as input darknet traffic and outputs inferred DNS amplification DRDoS insights. It is based on several components, namely, the flows generation, the detection, the rate classification and the clustering components. We discuss these components in what follows.

Flow Generation

The flow generation component takes as input darknet traffic to produce flows of traffic on a daily basis. A flow is defined as a series of consecutive packets sharing the same source IP address targeting darknet addresses. In order to generate such flow, we primarily collect network traces that consist of a unique source and destination IP pair, and then merge all flows that belong to the same source IP.

Detection Component

The detection component takes as input darknet traffic and outputs DNS-based DRDoS flows. To achieve the detection task, we base our detection component on analyzing DNS queries targeting darknet addresses. These DNS queries are attempts towards port 53. In order to detect DNS amplification DDoS, we built our approach in accordance with the parameters of Table 6.1. We describe below each of those parameters.

Parameter	**Value**
Packet Count	> 21 (experimental) > 29 (practical)
Targeted IPs	> 29
DNS Query Type	ANY
Requested Domain	Found in Root_DNS_DB

Table 6.1: DNS DRDoS Attacks Identification Parameters

- **Packet Count**: The packet count parameter defines the minimum number of packets sent per one source to our `/13` darknet space. This parameter is useful to extract DDoS attacks with high impact in addition to providing an estimate of its scale. For instance, a flow that possesses thousands of packets sent to darknet is larger and more effective than a flow with 50 packets. In order to estimate a suitable packet count parameter for the attack flows, we execute an experiment, as shown in Figure 6.2. The experiment is based on inferred darknet DDoS attacks and the investigation of their corresponding number of packets. For such attack flows, we fix the number of packets as perceived by the telescope and compute the number of attack flows that have at least such a number of packets. It is evident that below 21 packets, the attack flows will dramatically increase, while above that number, such flows will not decrease sharply. Thus, in this work, we decided to choose 21 packets as the packet count parameter for a DDoS attack flow. We assert that this threshold is a conservative number between false positives and false negatives. It is very significant to note that in [262], the authors also perform such experiment to extract DDoS attack flows; they found that 25 packets are suitable in their case, which was in 2006. We postulate that the slight decrease in packet threshold that we found is due to the recent rise of stealthy attacks that employ a lower number of packets per unit of time to achieve their attack while attempting to avoid detection.

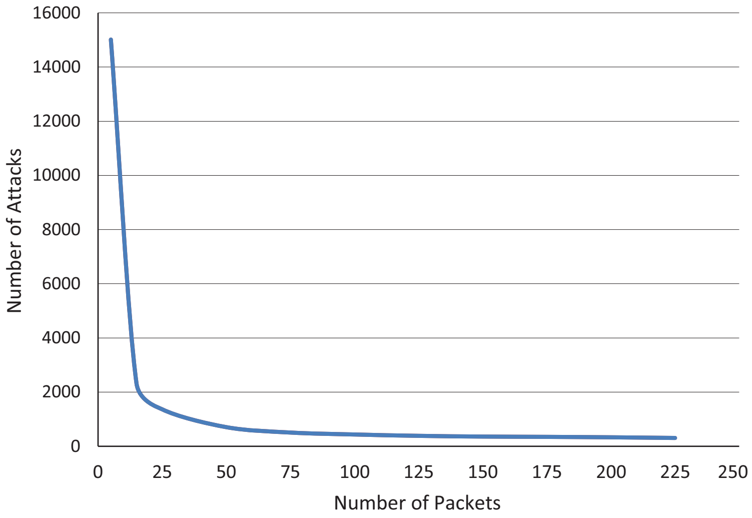

Figure 6.2: Packet Count Parameter Estimation

- **Targeted IPs**: Inspecting the number of targeted IPs verifies that the packets sent are not targeting only one IP address but distinct ones. Moreover, this permits the filtering of misconfiguration traffic (i.e., a host sending packets to only 1 unused IP address) and identifies the scanning mechanism for open DNS resolvers. To approximate a threshold for the number of targeted IPs, we semi-automatically (i.e., using a script and manual analysis and observation) investigated 1000 random DDoS attacks that were inferred by analyzing darknet using the open source network intrusion detection system Snort. The average of all those attacks were shown to target at least 29 different IPs. Thus, in this work, we assert that the inferred DDoS attempts involve at least 29 distinct open DNS resolvers. This is based on the realistic assumption that an attempt of contacting at least 29 unused IP addresses out of half a million darknet IP addresses in order to amplify an attack has a similar intention to contacting at least 29 distinct open resolvers on the Internet space. Please note that imposed by the latter, and in practice, one should adopt the minimum packet count to be at least 29 packets.

- **DNS Query Type**: One of the major strengths of DNS DDoS attacks is rendered by their amplification factor. In the majority of DNS amplification DDoS attacks, DNS query type `ANY` is used [282]. This type of DNS query returns all known information about a DNS zone in a single request to the victim. This technique is an attempt to amplify the attack. In this work, we impose that all DNS amplification DDoS traces have `ANY` as the DNS query type.

- **Requested Domain**: DNS amplification attempts are known to request root and Top Level Domain (TLD) name server operators [284]. We built a database containing a list of all known root and TLD domains. In general, these domains contain several DNS records. Therefore, DNS `ANY` queries targeting these servers trigger a large (amplified) reply. In this work, we corroborate that all DNS amplification DDoS activities request domains from the assembled database.

Note that we could have also added other parameters such as *attack-duration* and *packet-rate* to our detection component. However, we avoid using time-based constraints; we have detected some flash attempts [166] that targeted thousands of distinct unused IPs within seconds and other stealthy scanning activities [285] that persisted for several weeks.

In a nutshell, our detection component labels a flow of traffic as a DNS amplification DDoS attack if it has sent at least 21 DNS queries of type `ANY` to at least 29 distinct unused dark IP addresses. Further, the flow must have requested domains that exist in root and TLD database.

Rate Classification Component

The rate of the attack is one of the major characteristics of DDoS activities [262]. After inferring DNS amplification flows, we noticed the existence of a large deviation among DNS amplification DDoS attack rates. For example, some flow rates reached more than 50 thousand packets per second (pps) whereas others were below 1 pps. Therefore, in order to better understand this large deviation and to group attacks per attack rates, we executed a rate classification exercise based on the values found in Table 6.2. Please note that in order to compute the rate as well as the other parameters in Table 6.1, we employ a time-out metric, which is the case when a source in a particular flow ceases to send packets towards the network telescope.

Attack Rate Category	Value (pps)
Low	rate ≤ 0.5
Medium	$0.5 <$ rate < 4700
High	rate ≥ 4700

Table 6.2: Classification per Attack Rate

Going back to the rate classification procedure, the three attack rate categories are explained as follows:

- **Low Attack Rate**: To differentiate between low and medium attacks, we have executed an experiment with a number of confirmed attack flows as depicted in Figure 6.3. We also follow a conservative approach by choosing 0.5 pps as the threshold. Please note that the latter is only used to cluster the attacks per rate and thus is not employed in the detection component that was discussed in the previous section.

- **High Attack Rate**: This category contains high rate attempts that are commonly referred to as flash attacks [166]. We have chosen a threshold of 4700

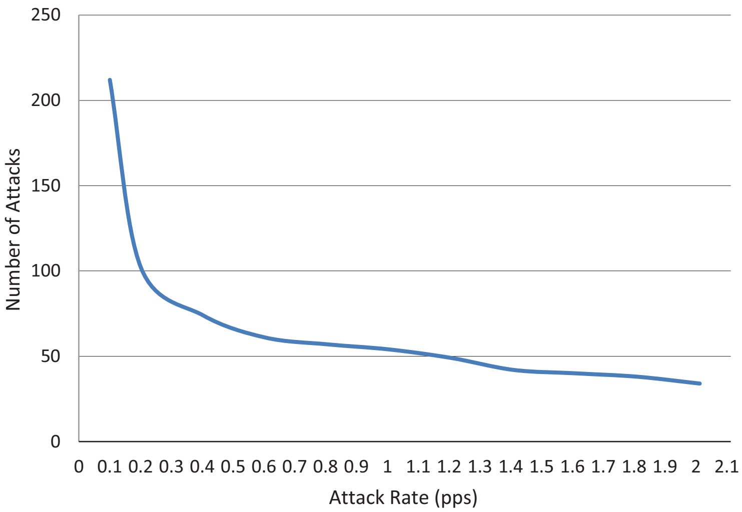

Figure 6.3: Rate Threshold

pps, which is the average rate of the Slammer worm propagation [166], to differentiate between medium and high rate attacks. In this exercise, we assume that the average rate of the fastest worm propagation in 2003 will have, at least, similar rates as flash attacks in 2014. Please note that in general, on one hand, worm propagation performs scans for vulnerabilities on hosts in an attempt to exploit or infect the victims. On the other hand, in relation to DNS amplification DDoS attempts, the attackers generate, in only one step, similar attempts to infer open DNS resolvers and execute the amplification attack. Recall, that the latter technique does not aim at searching for a vulnerability to exploit, but instead sends benign DNS `ANY` queries to abuse open DNS resolvers in order to amplify the replies on the victims.

- **Medium Attack Rate**: Intuitively, this class captures those attacks that are in between the low and high rate categories.

Clustering Component

We resort to data mining clustering approaches in an attempt to uncover and cluster similar DNS amplification DDoS traces that might be executed by similar authors, code, botnet or campaign. This exercise can aid in detecting patterns, trends and links among attack traces. To achieve this task, we have selected and extracted a number of attributes, as shown and described in Table 6.3.

Attribute	**Description**
ip.flag	IP Flags
ip.flag.df	Don't fragment
ip.len	Total IP Length
ip.ttl	Time to live
udp.len	UDP Length
dns.count.add.rr	DNS Additional RRs
dns.qry.name	DNS Query Name
flow.avg.pkt.size	Average Packet Size
flow.attack.duration	Attack Duration
high.asn.numb	Autonomous System #

Table 6.3: Chosen Clustering Attributes

Indeed, we have initially analyzed hundreds of attributes from different network layers (i.e., IP/UDP/DNS) in addition to numerous flow-based features (i.e., attack duration, average packet size, etc.). However, we have leveraged a ranker [286] to evaluate the information gain of all the attributes and have chosen the top 10 as shown in Table 6.3. This allowed us to filter out those attributes that were not applicable or have no or low information gain.

In order to perform the clustering, we have leveraged two algorithms, namely, the Expectation Maximization (EM) [287] and the k-means [288].

The EM algorithm: This popular iterative refinement algorithm is a standard procedure for maximum likelihood estimation. This procedure has two stages; the first, which is the expectation step, is used to mine the association between current estimates of the parameters and the latent variables by calculating subsequent probabilities. The second step, which is the maximization step, is employed to update the parameters based on an expected complete data log-likelihood [289].

The k-means algorithm: One of the most well-known and commonly used clustering technique is the k-means. First, the algorithm randomly selects k of the objects (i.e., values of extracted attributes), each of which initially represents a cluster mean or center. As for the remaining objects, based on the cluster mean, they are allocated to the closest cluster. Consequently, the algorithm calculates the new mean for every cluster. This process continues through other iterations until the criterion function converges.

We have chosen the above mentioned algorithms for several reasons. In addition to being well-known in tackling the data clustering problem, the k-means algorithm has been successfully used to detect anomalies [290] and DDoS [291]. On the other side, the Expectation Maximization, which extends the k-means paradigm using a probabilistic approach, has also been leveraged in clustering attacks [292, 293] and has been shown to yield promising results. For more information regarding the inner workings of the aforementioned clustering algorithms, we kindly refer the reader to [256].

6.1.2 Empirical Evaluation

The evaluation is based on a real darknet dataset during a 6-month period between January and June, 2013. Our proposed amplification inference approach is capable of processing and inferring attacks in around 90 seconds per 20 GB of darknet traffic. The latter advocates that the proposed approach is practically viable in operational environments. In regards to our data mining exercises, our analysis is based on Weka [257], which is a data mining tool implemented in Java. We abide and closely follow the steps of our proposed approach that was discussed in Section 6.1.1 to elaborate on our analysis, which is based on three main elements, namely, the characterization, the insights generation and a case study. In total, our approach identified 134 DNS amplification DDoS attacks, including high-speed, medium and stealthy attacks (please refer to the Appendix).

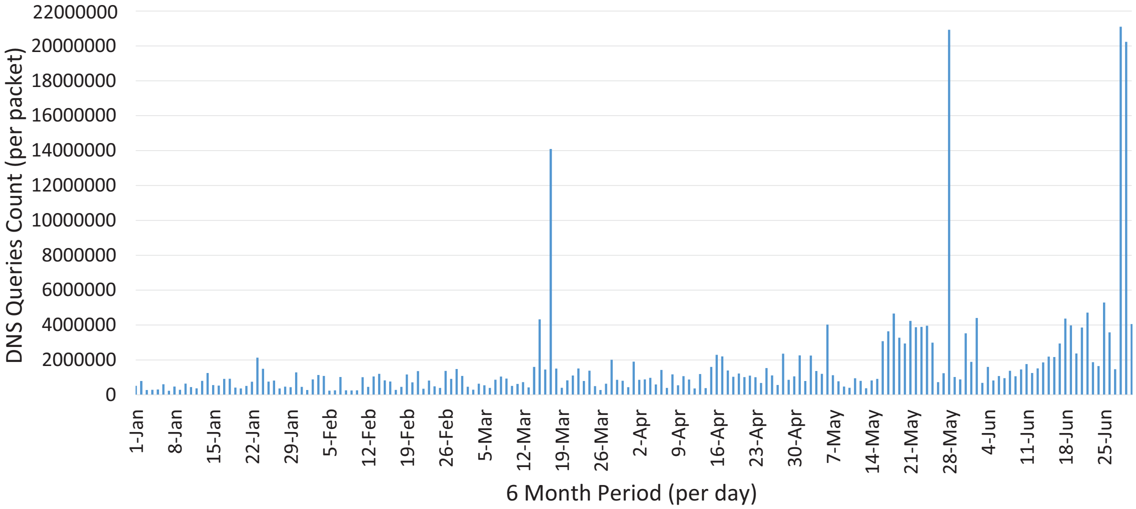

Figure 6.4: DNS Queries Distribution - Semi-annual 2013 Data

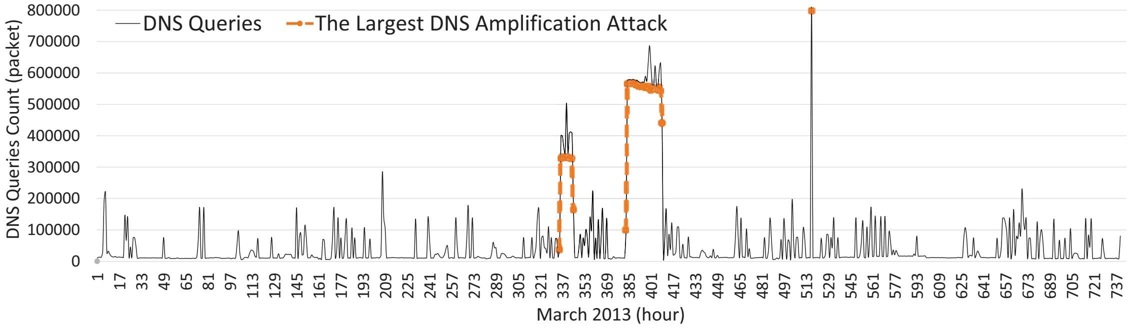

Figure 6.5: DNS Queries Distribution - March 2013 Data

DNS Amplification DDoS Characterization

In this section, we present the overall DNS amplification DDoS statistics related to our analyzed dataset. The semiannual DNS queries distribution is shown in Figure 6.4. The outcome clearly demonstrates the effectiveness of the proposed detection approach by fingerprinting large-scale reflection DDoS attacks including the famous reported event, which occurred in March 2013 [211]. On the other hand, in order to have a closer look at the latter attack, we depict Figure 6.5 that illustrates the distribution of the queries for the month of March. Please note that the other peaks which resemble various unreported reflection attacks, as shown in Figure 6.4, will be analyzed and elaborated in future work. The average DNS queries arrival time per hour is approximately 58050 packets. Obviously, several large-scale DNS reflection DDoS attacks caused some peaks at some periods such as at hours 340, 400 and 517, in which the distribution of packets was raised to 503995, 686774 and 798192 packets, respectively. More explanation on these peaks are discussed in Section 6.1.2.

Query Type Distribution: In order to understand the types of DNS queries received on the monitored dark space, we list in Table 6.4 the DNS query type distribution of the analyzed dataset. As expected, the vast majority of these requests are `ANY` queries. Note that the top 4 records are the same for the entire 6 months period. Further, in contrast with the results obtained in 2007 by [113] that found that `ANY` records scored only 0.0199% of the entire perceived records, we record 59.64% as observed on the darknet space. As a result, we can arguably assume that the recent trend of DNS amplification attacks are behind the increase of `ANY` records found on the darknet in the current year [211].

January **Packet_Count** **(%)**	**February** **Packet_Count** **(%)**	**March** **Packet_Count** **(%)**	**April** **Packet_Count** **(%)**	**May** **Packet_Count** **(%)**	**June** **Packet_Count** **(%)**
9717559 A (48.91%)	10047038 A (49.02%)	27649274 ANY (64.23%)	18378685 ANY (54.60%)	71798518 ANY (86.14%)	87174182 ANY (81.08%)
6738709 ANY (33.91%)	7763817 ANY (37.88%)	11310058 A (26.28%)	11595908 A (34.45%)	10966132 A (13.15%)	19876332 A (18.48%)
3323599 TXT (16.72%)	2479572 TXT (12.10%)	2459257 TXT (5.71%)	3402073 TXT (10.11%)	473973 TXT (0.56%)	410547 TXT (0.38%)
50473 MX (0.25%)	100463 MX (0.49%)	500143 MX (1.16%)	180779 MX (0.54%)	69117 MX (0.08%)	30130 AAAA (0.02%)
36438 PTR (0.18%)	29232 PTR (0.14%)	63340 RRSIG (0.15%)	28716 AAAA (0.09%)	37052 AAAA (0.04%)	15441 MX (0.01%)

Table 6.4: Top 5 DNS Query Type - 2013 Semiannual Darknet Data

Top Countries: Figure 6.6 and Figure 6.7 respectively show the top 5 source countries of DNS amplification DDoS attacks and their corresponding generated traffic. In what follows, we focus our analysis during the three months of February, March and April, 2013.

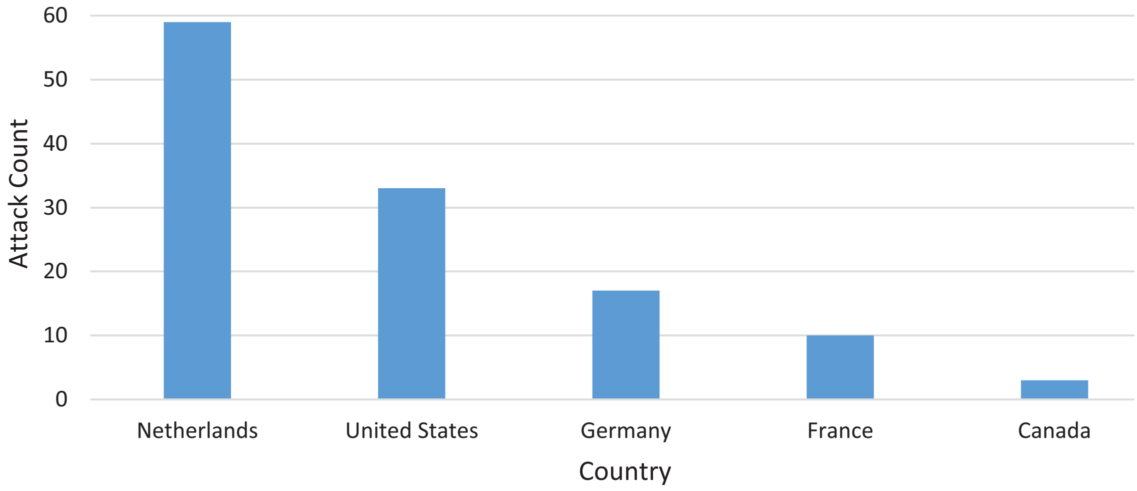

Figure 6.6: Top 5 Source Countries (Attacks)

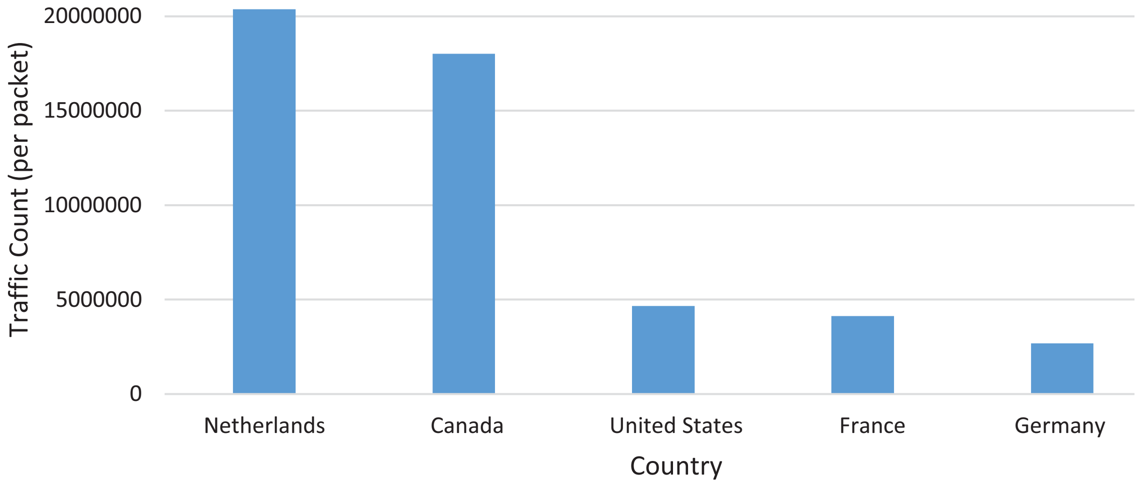

Figure 6.7: Top 5 Source Countries (Generated Traffic)

Note that Netherlands was ranked first in terms of both traffic sent and attack counts. Our results cross validate with the investigation in [294] and the news in [295]. Since Netherlands was mainly involved in the attack, it is normal to see victims and even scanners located in Netherlands. The United States was also found in our result as one of the top most involved countries. For Canada, notice the low number of attacks but the large amount of generated traffic. The reason behind this difference is that, although few of the Canadian IPs were involved, yet they generated a huge amount of traffic. This corroborates the fact that DNS reflection attacks are very powerful since they allow attackers to create an immense amount of traffic (i.e., the amplification factor) with very little effort (i.e., very small number of leveraged bots). After manual inspection, some of these Canadian IPs were found involved in the largest DDoS attack [18]. More on this result is discussed in Section 6.1.2.

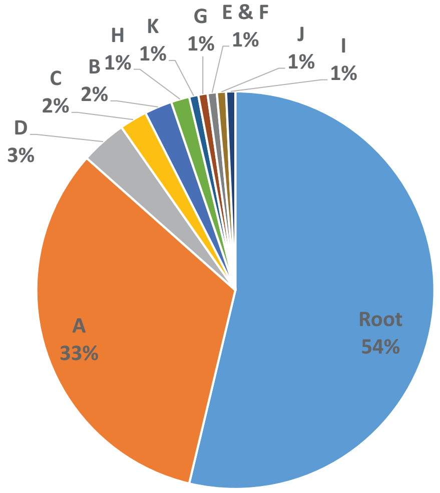

Figure 6.8: Top Requested Domains

Requested Domains: Last but not least, we illustrate the top requested DNS domains as shown in Figure 6.8. We anonymize TLDs for sensitivity issues. Figure 6.8 shows that `Root` is the most requested domain name as perceived by the monitored darknet. Recall that attackers will typically submit a request for as much zone information as possible to maximize the amplification effect. Hence, the use of `Root` as the requested domain name. Note that, from our data, the second top requested domain (labeled as A) is a TLD that belongs to a large Internet-scale DNS operator.

Clustering Insights

This section highlights our clustering results. Recall that the aim is to cluster similar DNS amplification DDoS traces that might be executed by similar authors, code, botnet or campaign.

Since we had no prior knowledge on the number of clusters, we first run the EM algorithm to only infer the number of clusters by cross validation [296]. We executed the algorithm in several cluster modes, using a training set and several percentage split tasks. We compared all the results and chose the model with the highest log likelihood for the best fit. After retrieving the number of clusters, we run the *k*-means with that number of clusters for further analysis. Again, we run several experiments (40%, 50%, 60%, 70% and 80% split) using the *k*-means algorithms and chose the model with 60% training data and 40% for testing as it achieved the minimum cluster sum of squared errors.

Cluster	***k*-means Instances**
0	31 (57%)
1	4 (7%)
2	12 (22%)
3	5 (9%)
4	2 (4%)

Table 6.5: *k*-means Clustered Instances

Based on our testing data, Table 6.5 lists our summarized instances per clusters while Figure 6.9 visualizes the final *k*-means output. Next, we disclose the attributes that formed the clusters. Table 6.6 shows the cluster centroids of the *k*-means algorithm. This table is based on the training set of the data.

It is shown that our model clustered the traces based on 4 different ASNs with some specific attributes. For instance, in regards to cluster 0, all the DDoS attacks have source IPs within `ASN-V` and have the `DF` flag not set in the IP header.

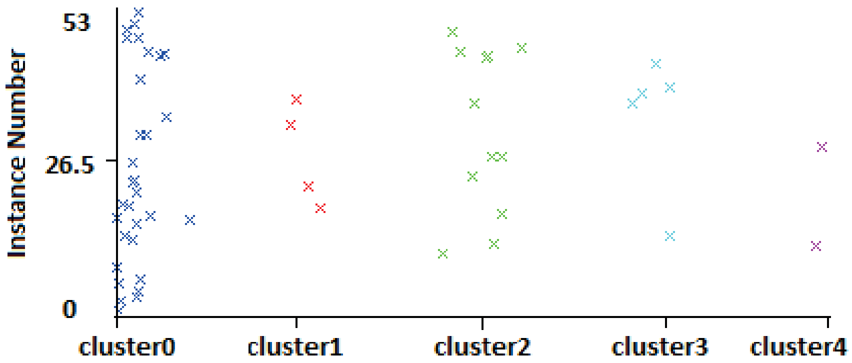

Figure 6.9: *k*-means Clustering of DNS Reflection DDoS attacks

Attribute	**Cluster 0 (49)**	**Cluster 1 (8)**	**Cluster 2 (14)**	**Cluster 3 (5)**	**Cluster 4 (4)**
high.asn.numb	ASN-V	ASN-W	ASN-X	ASN-Y	ASN-Y
ip.flag	0x02	0x00	0x02	0x00	0x02
ip.flags.df	0	1	0	1	0
ip.len	56	45	64	64	64
ip.ttl	<60	<60	<60	>100	<60
udp.length	36	34	44	44	44
dns.qry.name	Root	B	A	A	A
flow.avg.pkt.size	70	68	78	78	78
flow.attack.duration	<1day	<1day	<1day	<1day	btw-day-1week

Table 6.6: *k*-means Training Cluster Centroids

Moreover, the same flow must have an IP length of 56 bytes and a `TTL` value less than 60. In addition, the UDP length must be 36 bytes while the requested domain is `Root`. Additionally, all the attacks that belong to cluster 0 should be launched within a one-day period and possess an entire encapsulated DNS flow of an average packet size of 70 bytes. Through manual inspection, we found that the majority of IPs that fall within cluster 0 are originating from Netherlands, which is coherent with the investigation in [294]. A similar concept applies for other clusters. Note the similarities between clusters 2, 3 and 4 which could be the result of one campaign using different ASNs from different locations.

After the clustering exercise, in order to evaluate our model, we run the cluster evaluation algorithm in Weka [257]. First the algorithm ignores the class attribute and generates the clustering. Then it assigns classes to the clusters during the testing mode, based on the majority of values within each cluster. Afterwards, it calculates the classification error. Based on this technique, we have achieved a 82% accuracy. In other words, our model incorrectly classified 18% of the traces to their corresponding clusters. We aim, in our future work, to analyze more data and run more complex algorithms to improve our clustering result.

Please note that, although we do not have a decisive proof of whether each cluster represents a campaign or a botnet of DNS amplification DDoS, we relatively succeeded in this task by pinpointing similarities of features among the DNS amplification DDoS traces.

Similarity Insights

Next, we infer insights related to the used darknet address space. The aim is to provide a more core element to our clustering approach. The rationale behind this task states that since bots in the same campaign typically utilize the same list of IPs when launching their attacks, it would be interesting to capture the similarity related to the use of these IP lists. By accomplishing this task, we can possibly infer campaigns or at least detect similarities in attack mechanisms. To achieve the intended goal, we executed an experiment to represent attacks that exchange at least 90% of dark IPs. Figure 6.10 depicts an IP map[1] that satisfies the latter condition.

It is disclosed that two groups of IPs share at least 90% of dark IPs. Please refer to tables 7.1, 7.2 and 7.3 in the appendix for attack references. The smaller group consists of 2 IPs from different months (March and April). Our analysis identified that these two sources share not just dark IP usage, but also country, ASN number,

[1] The map was generated using Gephi [297], an open source visualization tool.

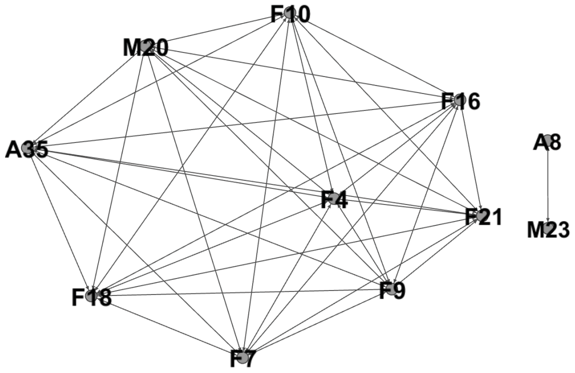

Figure 6.10: IPs Sharing at least 90% Darknet Space

speed range, requested domain, and many other attributes as previously identified in Section 6.1.2 in cluster 0. As for the second group, 7 out of 8 IPs originate from the same ASN number. All of the attacks in this group are initiated from Europe, specifically from Netherlands; this finding is corroborated in [294]. Similar to the first group, these attacks share similarities in clustering attributes and 55.56% of these traces are found also in cluster 0. One of the interesting point uncovered by analyzing this group is that all its members are sharing a specific address space range, possibly highlighting a DDoS campaign.

Case Studies

We discuss below some major case studies that belong to three different attack rates.

The first case study represents high-speed (i.e., flash) DNS amplification DDoS detected attacks. In our dataset, we have found 3 attacks that fall within this category, namely, ID F1, M1 and A1. These are shown in the first rows of Tables 7.1, 7.2 and 7.3, respectively. These attacks are found to be focused; intensity is equal to the contacted unique dark IPs or, in other words, the host/attacker sends only 1 packet per open DNS resolver. First, attack F1 is the fastest detected attack. It was launched from the United States, California on February 19th. The detected attack has a rate of 79565.67 pps. This propagation speed is 17 times faster than the Slammer worm [166]. This attack targeted 6.5% of our darknet in less than 1 second. Assuming the intent of the attacker is to send one packet for each IP, a malware with this speed can target the whole IPv4 Internet address space in less than a week (6 days and few hours). In order to validate the occurrence of this flash DNS reflection DDoS attack, we resorted to publicly accessible DShield [100] data and inspected port 53 for the 3 days before and after the 19th of February. We have noticed a significant increase at this specific date. According to DShield data, the average incident reports measured on port 53 was 14.28% for the surrounded 7 days of this attack. However, on February 19th, the average reached 38.19% with a 10347879 increase in reports from the previous day. Second, attack M1 was launched from Taiwan on March 18th. This date is the same for the largest DDoS attack as declared in [211]. This flash attack sent probes to 50257 unique dark IPs (9.5% of our /13 darkspace) within 1 second with an average rate of 46677.36 pps. This speed is almost 10 times faster than the Slammer worm. With this speed, this DDoS can target 16 millions IPv4 hosts (/8) on the Internet in less than 6 minutes. Third, attack A1 was also launched from the United States, California on April 15th. The attack possesses a rate of 21672.18 pps. This attack targeted 11.7% of our darknet address space.

The second case study, which involves medium speed attacks, is one of the major inferred DNS amplification DDoS in terms of size and impact. Compared to the previous case study, this attack is not focused (intensity is not equal to the contacted unique dark IP or sending at least 1 packet per open DNS resolver). This attack targeted one victim using 2 hosts (ID M5 and M10 of Table 7.2). This attack targeted around 360000 unique dark IPs (68% of the monitored /13 darknet), and hence could be considered the most comprehensive compared to all other threats. Our analysis linked these traces to the largest DNS amplification DDoS [18] for the following reasons: 1) In addition to the use of the ANY DNS query, the traces of this attack targeted the “ripe.net” domain, which was used in the largest DDoS attack as declared in a blog posted by the victim [211]; 2) the timing of the traces from the host with ID M10 started on March 15th, whereas those of the host with ID M5 started on March 17th. The two mentioned dates could be found in the media [298, 299] and were posted on Twitter on March 17th by a company support personnel [300]. In order to depict this distributed attack, in Figure 5.6, we highlight the threat using a colored dashed-line. The first and/or second peaks are likely performed as testing before actually executing the largest DDoS as demonstrated by the third peak. Our result matches the ascending order of peaks as discussed by the victims [211]. In order to predict or provide an approximation of the number of machines that were involved in the aforementioned largest DNS amplification attack, we assume the following: Consider M5 as a victim sample (spoofed IP or compromised machine). The average attempts sent on the darknet is 14464427 packets over 360705 open DNS resolvers which is around 40 requests per unique dark IP address. Recall that each dark IP might be considered as an open DNS resolver. Also, assume that the amplification factor is 75 [211] and each request has a size of 68 Bytes. Moreover, assuming only 1% (3607) of the 360705 requests reached successfully open DNS resolvers[2], then using a regular machine with a dedicated Internet service, only 1 host can generate amplified reply of 5.482 gigabits (Gb) through 3607 open DNS resolvers within 1 second. Therefore, to generate a 75 or 300 Gb DNS reflection DDoS attack, only 14 or 55 synchronized machines (bots) are needed, respectively.

The above two mentioned case studies are probably executed by an attacker using spoofed IP addresses of the victims or using compromised machines (recall Figures 2.2 and 2.3). We unlikely consider these activities as scanning events that are using legitimate addresses (i.e., the intention is not to attack themselves but other targeted victims).

The third case study involves slow rate attacks such as hosts with ID M51 to M54 in Table 7.2. This analysis targets stealthy focused attempts. These attacks have low sending rate and are typically hard to detect using a firewall and/or a

[2] As of November 2013, this is very probable as there is around 32 million open DNS servers on the entire Internet [301]

typical intrusion detection system [285]. From Table 7.2, all information regarding these 4 hosts appears very similar or the same. Therefore, such stealthy activities are mostly generated by the same author/code/campaign. Although we cannot claim the orchestration among these hosts, our data highlights some shared characteristics among such stealthy threats. Note that the requested domain names within these attacks belong to a well-known organization that deals with securing online transactions. Another group of stealthy attempts that are of interest are IDs `A48` and `A51` that are shown in Table 7.3. The hosts behind these activities scan slowly with an unprecedented average packet rate. For instance, ID `A48` remains online for almost 3 weeks. Future analysis on this group of stealthy attempts might pinpoint to certain suspicious unknown activities. Unfortunately, it is very hard to validate our stealthy scanning activities with other security repositories or media as their impact is in the information gain rather than the maliciousness of their acts. In contrast to the previous two case studies, the attackers in such stealthy scenarios can use their legitimate addresses. The reason behind this assumption is that it is almost impossible to execute a powerful DNS reflection DDoS attack through a low-speed propagation. However, in these attacks, we reason that attackers will attempt to locate open DNS resolvers and/or build a DNS hierarchy table retrieved from the `ANY` replies before executing their attacks.

In addition to performing several validations of our results through DShield and the media, we execute a renowned Network Intrusion and Detection System (NIDS) (i.e., Snort [41]) on the whole traces to see if we can detect such malicious activities. The NIDS labeled 129 out of the inferred 134 (96%) threats as executing filtered portsweep probes. We have found that the 5 undetected attacks refer to the third case study (i.e., slow rate attacks, namely, IDs `M51` to `M54` and `A51`) that was previously discussed. After manual inspection, the `M51` and `A51` attacks turned out to be originating from the same source that is executing stealthy scans but in different time periods. Moreover, all these attacks are requesting one organization's domain. In summary, we can claim that our approach that aims at inferring DNS reflection attacks yielded a zero false negative in comparison with a leading NIDS. Further, our approach, leveraging the darknet space, can infer DNS amplification DDoS activities while a NIDS is limited to pinpointing scanning activities.

6.2 Related Work

Cyber security experts and researchers employ darknet analysis for several purposes, namely, monitoring and inferring large-scale Internet events, including, DDoS [30], probing activities [9, 28], worm propagation [46], analyzing events [196], measuring misconfiguration [1] and implementing monitoring sensors [57]. Since this part of the thesis deals with cyber threats characterization in general and amplification DDoS in particular, we subsequently pinpoint the relevant related work in the areas of darknet profiling, DDoS attacks and darknet analysis, and amplification analysis.

Profiling darknet data: Pang et al. [108] elaborated on a detailed analysis of darknet data. Their active and passive analysis assessed darknet samples from different networks over a long period of time. Four years later, Wustrow et al. [2] reviewed the last mentioned work to update the state of this Internet background radiation. The authors observed significant changes and pinpointed several factors that are behind these measures. Moreover, Fukuda et al. [258] studied correlations among darknet traffic for estimating their behaviors through small address blocks by analyzing a specific type of traffic packets (i.e., TCP SYN). Furthermore, Oberheide et al. [113] analyzed specific services on darknet such DNS. The authors characterized these traces and proposed a mechanism to implement a secure DNS service on darknet sensors. In another work, Dagon et al. [284] analyzed corrupted DNS resolution paths and pinpointed an increase in malware that modified these paths and threatened DNS authorities.

DDoS attacks and darknet analysis: The use of darknet to infer DDoS activities owes much to the pioneer work carried out by Moore et al. [30] that was revisited in [262]. The key observation behind the authors' technique is that attackers, before executing a DDoS attack, spoof their addresses using random IP addresses. As such, all victims' replies (i.e., backscattered packets) are bounced back to the fake IP addresses, which could be in the monitored darknet. Their work is operated by CAIDA [302], which provide backscattered data for researchers. Numerous research works have been performed on such data to analyze DDoS activities. The majority focus on implementing new detection techniques to infer DDoS attacks [120,154,155,213], tracing-back the sources of attacks [42,303], investigating spoofed attacks [195] and visualizing attacks [225,304,305]. Further, very recently, Wang et al. [306] have executed a large empirical study on Botnet-based DDoS activities. Their work investigated data generated through active and passive measurements from several countries. Some of their findings include insights on the geo-spatial distribution and co-occurrence of orchestrated attacks against similar victims.

Amplification analysis: Paxson [209] was among the first to pinpoint the threats of DNS reflectors. The author discussed various defenses against reflector attacks and indicated three types of threats abusing network services, namely, DNS, Gnutella and web servers via TCP. Rossow et al. [32] revisited UDP-based protocols that can be abused for reflection attacks. The authors identified 14 protocols that are susceptible to DRDoS amplification. Similarly, Kuhrer et al. [210] demonstrated that even TCP protocols can be abused for amplification. In an another work, Anagnostopoulos et al. [283] introduced a new technique to execute DNS amplification attacks through DNSSEC-powered servers. Moreover, Czyz et al. [242] characterized NTP traffic and reflection attacks on darknet and showed the rise and decline of NTP DRDoS attacks using a large empirical study.

Our work is complementary and extends the aforementioned research works by exploiting requests (i.e., query) packets targeting the darknet to effectively infer DRDoS amplification activities. In this work, we do not only focus on the measurement and characterization of amplification attacks, but also uncover their attack meachnisms throughout darknet analysis.

6.3 Summary

In this chapter, we presented a novel approach to infer Internet DRDoS activities by leveraging the darknet space. The approach corroborated the fact that one can infer DDoS attacks without relying on backscattered analysis. The detection module was based on certain parameters to fingerprint network flows as DNS amplification DDoS-related. The classification module amalgamated the attacks based on their possessed rate while the clustering component attempted to identify flows that share similarity features to disclose campaigns of DRDoS. The analysis was based on 1.44 TB of real darknet traffic collected during a several month period. The results disclosed 134 DNS reflection DDoS activities, including flash and stealthy attacks. The clustering and similarity exercises provided insights and inferences that permit the detection of DNS amplification DDoS campaign activities. Moreover, the discussed case studies elaborated on three attack categories and provided significant related cyber security intelligence.

Lessons Learned and Future Work

From this work, we can extract the following insights related to DNS amplification attacks. First, when compared to previous years, we have found that DNS amplification attacks are behind the increase of DNS queries of type `ANY` on the Internet. Second, we have pinpointed that the majority of the attacks target the root domain.

Third, we have inferred that DNS reflection attack rates can range from very low to high speeds. High speed attacks pinpoint victims of spoofed attacks and compromised machines whereas the very slow attacks reflect stealthy scans. Last but not least, we have unexpectedly uncovered a UDP-based mechanism used by attackers to execute DNS amplification attacks in a highly rapid manner without collecting information about open DNS resolvers. In other words, we have inferred that unlike typical DDoS attempts that scan for vulnerable machines and then execute the attack, the largest DNS amplification analyzed was executed in only one step through a small number of machines; benign DNS queries are sent to the Internet with the intention to reach open DNS resolvers, which subsequently trigger a reflection reply to the victim.

As for future work, we aim to execute our model on a larger data set and experiment with more complex data mining exercises to improve our clustering model.

Chapter 7

Conclusion

Technology has emerged in all aspects of our lives. Regrettably, adversaries are abusing technology for their own benefits. As a result, Internet services have become a cheap tool for attackers to generate malicious activities such as infecting victims' machines, taking control, exhausting resources and stealing information.

Recent events demonstrated that individuals, corporations and governmental organizations could be subjected, at the speed of light and in full anonymity, to amplified, large-scale and disrupting attacks that might lead to severe privacy/security and economic consequences, and even to the endangerment and loss of human lives. DoS attacks are perhaps the most prominent and severe types of such large-scale cyber attacks. These attacks might be carried out by a spectrum of individuals such as criminals, cyber-terrorists and foreign government spies. Moreover, as the closest approximation of perfect anarchy, the Internet becomes an attractive tool to terrorists for spreading messages, recruiting supporters, planning and coordinating attacks. In this context, it is a national duty of paramount importance to monitor and protect Internet services.

In this thesis, we tackled the increasing cyber security concern rendered by

DoS activities. To achieve this task, we successfully monitored darknet, also known as network telescope. In particular, we primarily reviewed the literature in terms of darknet deployment approaches, analysis techniques and visualization of its data. Darknet projects were found to monitor various cyber threat activities and were distributed in one third of the global Internet. We further identified that Honeyd is probably the most practical tool to implement darknet sensors, and future deployment of darknet will include mobile-based VOIP technology. In addition, as far as darknet analysis is considered, computer worms and scanning activities were found to be the most common threats that can be investigated throughout darknet. Code Red and Slammer/Sapphire are the most analyzed worms. Furthermore, our study uncovered various lacks in darknet research. For instance, less than 1% of the contributions tackled DRDoS amplification investigations and at most 2% of research works pinpointed spoofing activities. Second, we studied the nature of darknet data and the correlation among inferred threats. Such work proved that specific darknet threats are correlated. Moreover, it provided insights about threat patterns and allowed the interpretation of threat scenarios. Third, we attempted to predict DoS events by proposing a forecasting model. The extracted inferences from various DDoS case studies exhibited a promising accuracy with low error rate. Further, our prediction model could lead to a better understanding of the scale, speed and size of DDoS attacks and generates inferences that could be adopted for immediate response and mitigation. Moreover, the accumulated insights could be used for the purpose of long term large-scale DDoS analysis. Finally, we concentrated our research work towards the detection of large-scale DDoS activities. While inferring such malicious activities, we uncovered traces from the largest DNS amplification attack in history, and consequently proposed a novel approach to fingerprint and estimate the size of amplification attacks. Complementary to the pioneer work on inferring DDoS activities using darknet, this work proved that we can extract DDoS activities without relying on backscattered analysis. The results uncovered high-speed and stealthy attempts that were never previously documented. The extracted insights from various validated DNS DRDoS case studies led to a better understanding of the nature and scale of this threat and generated inferences that could contribute in detecting, preventing, assessing, mitigating and even attributing DRDoS activities.

From the conducted research, we have extracted the following points:

- Compared with other trap-based monitoring systems, darknet is considered as a practical and easy-to-implement tool in passive monitoring the cyber space. Darknet setup can be developed using basic routing techniques and can be monitored through IDSs.

- Mobile darknet is a new trend that has a promising future in passive monitoring research. The future deployment will include mobile-based VoIP darknet.

- A study in 2001 [126] shows that darknet sensors occupy 5% of the whole IPv4 address space. An up-to-date study is needed to approximate the current size of darknet.

- Filtering darknet misconfiguration is still not thoroughly investigated in the literature and hence requires more attention from the research community.

- Inferring and attributing botnet or malicious campaigns by solely monitoring darknet is challenging due to the passive nature of such IP space. Therefore, other interactive techniques such as honeypots could be used in conjunction with darknet analysis to enhance botnet investigation.

- IPv6 darknet, event monitoring and game engine visualization methods require a significantly greater amount of attention from the research community.

- Differentiating between scanning and DRDoS is still partially a difficult problem due to the fact that both leverage scan-based techniques to operate. Scanning activities probe the Internet to collect information, whereas reflection activities generate scan-based requests to redirect amplified reply traffic to victim.

- Packet analysis is the only technique used on darknet data to investigate spoofing activities. This method includes inspecting ICMP packets and TTL values. Based on our survey, less than 2% of research has been done on spoofing and darknet. Therefore, spoofing is still a severe malicious activity that needs more attention from the security research community.

- Despite the existence of some collaborative darknet projects, more darknet resources and information sharing must emerge to infer and attribute large-scale cyber activities. Dealing with a worldwide darknet information exchange is a capability that requires collaboration and trust; however, this collaboration raises security policies and privacy concerns.

7.1 Discussions

We list below some of the most relevant topics for discussion.

- **Analysis of IPv4 & IPv6 Darknet Data:** A major element that distinguishes IPv4 from IPv6 is the size of the address space. In a nutshell, IPv6 is designed to provide significantly more address space to handle the Internet growth in a more secure and efficient manner. The migration and integration between these two technologies have already started [307]. For instance, several techniques are being leveraged to handle this migration such as tunneling and address translation. This shift will obviously affect network monitoring systems such as darknet. As such, both defense and attack mechanisms will be affected. For instance, in regard to security, IPv6 packets might have higher encryption. The latter will make it harder for defense teams to analyze and interpret suspicious traffic and easier for attackers to obfuscate. Furthermore, since IPv6 is larger in address space, this will make it harder to monitor huge amounts of traffic. It is also difficult for attackers to probe the large address space to look for vulnerabilities. Regardless of the aforementioned impacts, it is only a matter of time for IPv6 darknet to become more involved in the era of trap-based monitoring system. This requires attention from the security community.

- **Deployment and Technology Development:** Nowadays, technology has become a part of our daily life. Basic electronic devices such as phones, watches, and glasses have evolved into smart equipment and become easily accessible through the Internet. This new shift has obviously increased the opportunity for malicious users to abuse such services. The latter threat can have a direct impact on our lives. For instance, attackers are abusing the Internet to generate flood of Voice over IP phone calls to attack 911 emergency phone services or spam mobiles with anonymous call or SMS messages [50]. Therefore, deploying darknet and honeypot sensors that operate on phone and mobile numbers is highly needed. The latter techniques are considered significantly important and require enormous attention from the research community.

- **Visualization and Learning:** Today's revolutionary technology is putting emphasis on visualization for the simple and friendly use of machines and information. In fact, researchers have found that, in a learning environment, the majority of people need to see information before learning [308]. As such, visualization and gaming have emerged largely in technologies such as social media, mobile and web services. In regard to cyber security, our vision is coherent with some of the aforementioned research works in [218–220], which emphasize on building monitoring systems based on game engines and visualization techniques. Therefore, we believe that the future generation of tools and technologies in cyber security will include more visual effects and game-based services. Such technologies already exist. For instance, the LOIC [309] is a well-known network stress testing and DDoS attack tool used by malicious and benign users in a game-friendly manner. We predict that, in the upcoming years, similar technologies will become a new trend for the cyber space.

- **Cyber Capabilities:** One of today's challenges is to build cyber capabilities with the ability to provide a generic technique to automate the inference of botnet and orchestrated campaigns (i.e., DDoS and Spamming). The NICTER project [77] is a typical scenario of such cyber capability. Moreover, another challenge is to build a trusted centralized repository of darknet data that can be used for worldwide monitoring and intelligence sharing. Such a worldwide project requires a thorough understanding of the challenges behind the privacy and legal issues.

- **Cyber Awareness:** Enforcing cyber laws has escalated the intensity of attacks [310]. Therefore, cyber law enforcement and its related security technologies are not the ultimate solution to mitigate and defend against cyber attacks. As such, other techniques like learning and education are needed to increase the awareness and help in applying best practices for ethically using the cyber space as a service instead of abusing its enormous capabilities.

7.2 Considerations

In general, our overall proposed approaches leverage darknet to infer and extrapolate attacks. Therefore, there are three assumptions that underlie our analysis:

- **Attackers' IP Address Selection:** Although our monitored sensors are relatively large (i.e., `/13`), the approach is unable to monitor events that do not target such sensors. The latter can occur when attackers use an already published hit list or test specific and known amplifiers. Although such methods will allow attacks to avoid being detected or assessed by our approach, adversaries in general prefer to employ an up-to-date and various hit lists of amplifiers to decrease their chances of being detected and to increase their chances of launching amplification attacks [32]. To achieve the latter, at least one global scan is first needed to assess the impact of the amplification factor; a scan that would probably hit our sensors. We concur that we are not aware of any worldwide reported attacks that were not (at least partially) inferred by our proposed approach.
- **Detection Avoidance:** Our proposed detection algorithm leverages several attack parameters. As such, attackers can tune their attacks to avoid being detected. For instance, adversaries can craft raw IP packets or inject random delays to reduce the flow to a rate below the employed threshold parameter. However, we argue that crafting raw IP packets and injecting random delay in the attack flows are relatively time consuming operations, especially given that one of the major amplification attack parameters is the rate. Thus, attackers adopting these methods will decrease their efficiency or at least reduce the impact of their generated attacks.

7.3 Future Work

The investigation of DRDoS activities has seen increasing attention from the security community in terms of measurement and analysis [32]. However, the issue of how to systematically assess the impact of such attacks on the Internet infrastructure has not yet been dealt with. The latter task becomes even more imperative, given that current practices rely on manual and reactive analysis. For instance, the largest Domain Name System (DNS) DRDoS attack that occurred in 2013 required more than few days to be analyzed [211], where its actual impact was speculated to range between 75 Gbps [40] and 300 Gbps [211]. Further, the analysis of the largest Network Time Protocol (NTP) DRDoS attack of 2014 took more than 3 days [5], where its actual rate and impact were postulated a week later. Additionally, while investigating thousands of DDoS and DRDoS activities for several years, we have discovered that labeling some large-scale DDoS attacks as severe, based solely on the number of packets, could lead to inaccurate results or even false positives. Therefore, as future work, we aim at tackling the design and implementation of a prediction model for amplification attacks.

APPENDIX

The summary of the Analyzed DNS Amplification DDoS Traces of February, March and April 2013 is shown in Table 7.1, 7.2 and 7.3 respectively.

Victim/ Scanner ID	**Requested Domain Name**	**Detection Period**	**Analyzed Attack Duration (second)**	**Intensity (packet)**	**Contacted Unique Dark IPs**	**Avg. Packet Size (Bytes)**	**Avg. Rate (pps)**	**Rate Category**
F1	A	Feb 19	0	34410	34410	78	79565.67	High
F2	G	Feb 14	4477	129206	129206	85	28.86	Medium
F3	A	Feb 21	29174	690219	305544	78	23.66	Medium
F4	Root	Feb 26	17084	351617	351617	70	20.58	Medium
F5	Root	Feb 19	16245	290590	290590	70	17.89	Medium
F6	Root	Feb 26	9389	162513	162513	70	17.31	Medium
F7	Root	Feb 11-12	25052	349692	349692	70	13.96	Medium
F8	Root	Feb 20	15215	187886	187886	70	12.35	Medium
F9	Root	Feb 13	61591	660473	356162	70	10.72	Medium
F10	Root	Feb 16-17	33602	355188	355188	70	10.57	Medium
F11	Root	Feb 3	6625	64726	64726	70	9.8	Medium
F12	Root	Feb 23	11412	96216	96216	70	8.4	Medium
F13	Root	Feb 2-3	93268	633886	357497	70	6.8	Medium
F14	A	Feb 3	19872	128297	128297	78	6.46	Medium
F15	Root	Feb 7	2107	12965	12965	70	6.15	Medium
F16	Root	Feb 23-27	401266	804348	359868	70	2	Medium
F17	Root	Feb 11-15	311301	316425	316425	70	1.02	Medium
F18	Root	Feb 4-19	1322119	869395	360666	70	0.66	Medium
F19	Root	Feb 4-14	853983	540412	356117	70	0.63	Medium
F20	A	Feb 3	10634	6632	6632	78	0.62	Medium
F21	A	Feb 3-16	1138804	683321	359470	78	0.6	Medium
F22	Root	Feb 20-28	766810	378289	319668	70	0.49	Low
F23	Root	Feb 5	27832	9645	8123	70	0.35	Low
F24	A	Feb 19	50374	16393	16393	78	0.33	Low
F25	A	Feb 4	16353	5306	5306	78	0.32	Low
F26	Root	Feb 6-26	1706728	191562	191329	70	0.11	Low
F27	Root	Feb 15-26	970150	19636	19636	70	0.02	Low
F28	A	Feb 9-28	1691139	16845	16845	78	0.01	Low
F29	A	Feb 15-22	640165	966	966	78	0	Low

Table 7.1: Summary of DNS Amplification DDoS Traces (February 2013)

Victim/ Scanner ID	Requested Domain Name	Detection Period	Analyzed Attack Duration (second)	Intensity (packet)	Contacted Unique Dark IPs	Avg. Packet Size (Bytes)	Avg. Rate (pps)	Rate Category
M1	A	March 18	1	50257	50257	78.00	46677.36	High
M2	A	March 31	26	63543	63543	78.00	2419.83	Medium
M3	E & F	March 22	620	798192	65025	73.00	1287.41	Medium
M4	A	March 20	402	91042	91042	67.00	226.21	Medium
M5	B	March 17-18	93508	14464427	360705	68.00	154.69	Medium
M6	Root	March 3	572	64956	64956	70.00	113.53	Medium
M7	Root	March 23	662	64230	64230	70.00	97.00	Medium
M8	Root	March 30	610	58104	58104	70.00	95.19	Medium
M9	Root	March 24	665	63139	63139	70.00	94.99	Medium
M10	B	March 15	34605	3176785	360683	68.00	91.80	Medium
M11	Root	March 1	769	63342	63342	70.00	82.33	Medium
M12	A	March 25	985	79333	54632	78.00	80.52	Medium
M13	Root	March 12	581	40364	37160	70.00	69.46	Medium
M14	Root	March 1-2	2685	161847	154905	70.00	60.28	Medium
M15	C	March 25	1	60	60	77.00	58.69	Medium
M16	A	March 9	8884	504794	270352	78.00	56.82	Medium
M17	A	March 30	1963	63623	63623	78.00	32.41	Medium
M18	Root	March 21	10255	254285	254285	70.00	24.80	Medium
M19	Root	March 7	13572	247483	247483	70.00	18.23	Medium
M20	Root	March 2	25314	355675	355675	70.00	14.05	Medium
M21	Root	March 13	9796	128147	128147	70.00	13.08	Medium
M22	Root	March 27	24391	286664	286664	70.00	11.75	Medium
M23	Root	March 8	33354	346244	346244	70.00	10.38	Medium
M24	Root	March 28-29	33280	342941	342941	70.00	10.30	Medium
M25	A	March 17-18	71943	358931	267826	78.00	4.99	Medium
M26	A	March 30	13667	61269	51999	78.00	4.48	Medium
M27	Root	March 14-17	342024	1396535	360701	70.00	4.08	Medium
M28	Root	March 28-29	56305	224327	224327	70.00	3.98	Medium
M29	Root	March 11	73864	248582	129708	70.00	3.37	Medium
M30	A	March 24	213	663	663	78.00	3.12	Medium
M31	Root	March 28-29	85385	221213	221213	70.00	2.59	Medium
M32	A	March 30	163	397	396	78.00	2.43	Medium
M33	A	March 29-30	82278	159295	159295	78.00	1.94	Medium
M34	A	March 30	330	640	639	78.00	1.94	Medium
M35	Root	March 24-25	69590	127214	127214	70.00	1.83	Medium
M36	A	March 31	38596	63553	63311	78.00	1.65	Medium
M37	Root	March 21-24	182116	254529	130964	60.00	1.40	Medium
M38	Root	March 4-5	140455	184555	159959	70.00	1.31	Medium
M39	Root	March 22-25	276510	352012	352011	70.00	1.27	Medium
M40	Root	March 22-23	116870	118871	65213	70.00	1.02	Medium
M41	Root	March 15-29	1207792	1171393	360697	70.00	0.97	Medium
M42	Root	March 22-29	563031	404882	351862	70.00	0.72	Medium
M43	A	March 1	21616	7107	7107	78.00	0.33	Low
M44	A	March 15	52584	17013	17013	78.00	0.32	Low
M45	A	March 1-7	466136	92176	89073	78.00	0.20	Low
M46	A	March 15-31	1393227	152254	134270	78.00	0.11	Low
M47	A	March 6-30	2119713	194209	65792	78.00	0.09	Low
M48	A	March 13	24521	2297	2117	78.00	0.09	Low
M49	Root	March 6-24	1570323	64062	63698	70.00	0.04	Low
M50	A	March 18-28	642350	278	236	78.00	0.00	Low
M51	D	March 27-28	41548	44	44	70.00	0.00	Low
M52	D	March 27-28	75803	42	42	70.00	0.00	Low
M53	D	March 27-28	90128	39	39	70.00	0.00	Low
M54	D	March 27-28	56874	37	37	70.00	0.00	Low

Table 7.2: Summary of DNS Amplification DDoS Traces (March 2013)

Victim/ Scanner ID	Requested Domain Name	Detection Period	Analyzed Attack Duration (second)	Intensity (packet)	Contacted Unique Dark IPs	Avg. Packet Size (Bytes)	Avg. Rate (pps)	Rate Category
A1	A	Apr 15	3	61859	61859	78	21672.18	High
A2	H	Apr 13	136	64485	64485	70	472.64	Medium
A3	Root	Apr 10	70	18718	18718	70	266.8	Medium
A4	A	Apr 21	4463	479863	264283	78	107.51	Medium
A5	Root	Apr 25	4023	151894	151894	70	37.76	Medium
A6	Root	Apr 20	325	11068	11068	70	34.05	Medium
A7	C	Apr 28	1274	40903	40903	77	32.11	Medium
A8	Root	Apr 4	6927	218917	218917	70	31.6	Medium
A9	Root	Apr 25	3171	57837	42578	70	18.24	Medium
A10	A	Apr 4	3791	68039	56211	78	17.95	Medium
A11	Root	Apr 16	8723	154154	154154	70	17.67	Medium
A12	Root	Apr 11	24015	350275	350275	70	14.59	Medium
A13	I	Apr 1	23608	340905	340905	92	14.44	Medium
A14	Root	Apr 25	39305	408596	408596	70	10.4	Medium
A15	Root	Apr 16-17	27760	284387	284386	70	10.24	Medium
A16	Root	Apr 12	6821	64299	64299	70	9.43	Medium
A17	Root	Apr 16-17	65224	610166	355290	70	9.35	Medium
A18	Root	Apr 13-14	11834	95117	95117	70	8.04	Medium
A19	B	Apr 5-6	73456	345133	343652	79	4.7	Medium
A20	Root	Apr 14-15	42560	182836	182834	60	4.3	Medium
A21	A	Apr 20-21	55680	237640	190915	67	4.27	Medium
A22	Root	Apr 6-8	179271	695695	360267	60	3.88	Medium
A23	A	Apr 15-16	89471	346554	346554	78	3.87	Medium
A24	Root	Apr 1-2	135389	507427	291844	70	3.75	Medium
A25	A	Apr 18	23	85	85	78	3.75	Medium
A26	A	Apr 24-30	568658	1601134	357930	78	2.82	Medium
A27	Root	Apr 1-2	120727	316718	224789	70	2.62	Medium
A28	A	Apr 21	46328	116129	65563	78	2.51	Medium
A29	Root	Apr 2-3	90532	222416	222416	70	2.46	Medium
A30	Root	Apr 13-15	184882	408581	228422	70	2.21	Medium
A31	Root	Apr 22-23	145929	321446	257906	70	2.2	Medium
A32	A	Apr 3-4	56113	120662	120662	78	2.15	Medium
A33	Root	Apr 1-29	2463203	3495104	360705	70	1.42	Medium
A34	Root	Apr 13-22	777630	1049946	360690	70	1.35	Medium
A35	Root	Apr 3-8	463324	593142	357414	70	1.28	Medium
A36	Root	Apr 7-11	295595	316685	225376	70	1.07	Medium
A37	A	Apr 10-20	839737	746958	297831	78	0.89	Medium
A38	Root	Apr 27-28	91306	64338	64338	70	0.7	Medium
A39	A	Apr 12	18587	6049	6049	78	0.33	Low
A40	A	Apr 5-20	1312707	385495	65792	78	0.29	Low
A41	A	Apr 25-30	431330	119938	65642	78	0.28	Low
A42	C	Apr 17-19	158580	40362	40362	77	0.25	Low
A43	Root	Apr 13-20	543326	129962	95477	70	0.24	Low
A44	A	Apr 1-4	288469	60878	60878	78	0.21	Low
A45	A	Apr 17-26	831476	131106	109673	78	0.16	Low
A46	Root	Apr 14-20	496168	63559	40901	70	0.13	Low
A47	Root	Apr 5-10	426625	35125	35125	70	0.08	Low
A48	J	Apr 2-23	1828890	81868	3744	75.49	0.04	Low
A49	H	Apr 9-10	96970	1077	1074	70	0.01	Low
A50	K	Apr 23-30	640451	8964	7871	68	0.01	Low
A51	D	Apr 15-17	156226	63	47	71.02	0	Low

Table 7.3: Summary of DNS Amplification DDoS Traces (April 2013)

Bibliography

[1] M. Bailey, E. Cooke, F. Jahanian, A. Myrick, and S. Sinha, "Practical darknet measurement," in *40th Annual Conference on Information Sciences and Systems*. IEEE, 2006, pp. 1496–1501.

[2] E. Wustrow, M. Karir, M. Bailey, F. Jahanian, and G. Huston, "Internet background radiation revisited," in *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*. ACM, 2010, pp. 62–74.

[3] BBC News, "Stuxnet worm: targeted high-value Iranian assets," http://www.bbc.co.uk/news/technology-11388018, last accessed in October 2015.

[4] News by BBC. Flame: Massive cyber-attack discovered, researchers say. http://www.bbc.com/news/technology-18238326. Last accessed in October 2015.

[5] CloudFlare. Technical Details Behind a 400 Gbps NTP Amplification DDoS Attack. http://tinyurl.com/p3exvnc. Last accessed in October 2015.

[6] Federal Bureau of Investigation, "Testimony - Taking Down Botnets," http://www.fbi.gov/news/testimony/taking-down-botnets, last accessed October 2015.

[7] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *Communications Magazine, IEEE*, vol. 51, no. 1, pp. 42–49, January 2013.

[8] C. Fachkha and M. Debbabi, “Darknet as a source of cyber intelligence: Survey, taxonomy and characterization,” *IEEE Communications Surveys and Tutorials*, vol. PP, no. 99, pp. 1–1, 2015.

[9] S. Bellovin, “There be dragons.” in *USENIX Summer*, 1992.

[10] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, “Inferring Internet denial-of-service activity,” *ACM Transactions on Computer Systems (TOCS)*, vol. 24, no. 2, pp. 115–139, 2006.

[11] A. Dainotti, R. Amman, E. Aben, and K. C. Claffy, “Extracting benefit from harm: using malware pollution to analyze the impact of political and geophysical events on the internet,” *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 1, pp. 31–39, 2012.

[12] E. Cooke, M. Bailey, Z. M. Mao, D. Watson, F. Jahanian, and D. McPherson, “Toward understanding distributed blackhole placement,” in *Proceedings of the 2004 ACM workshop on Rapid malcode.* ACM, 2004, pp. 54–64.

[13] Arbor Networks. 2012 Infrastructure Security Report. Last accessed in October 2015. [Online]. Available: http://tinyurl.com/ag6tht4

[14] ArborNetworks, “ATLAS,” http://atlas.arbor.net/, last accessed in October 2015.

[15] Forbes. Testing The Limits, LulzSec Takes Down CIA’s Website. Last accessed in October 2015. [Online]. Available: http://tinyurl.com/bfhzbta

[16] PcWorld. Hacker Arrested for DDoS Attacks on Amazon.com. Last accessed in October 2015. [Online]. Available: http://tinyurl.com/d22myng

[17] ITPRO. InfoSec 2011: Energy firms pummelled by DDoS attacks. Last accessed in October 2015. [Online]. Available: http://tinyurl.com/cpqodbx

[18] Ars Technica. When spammers go to war: Behind the Spamhaus DDoS. Last accessed in October 2015. [Online]. Available: http://tinyurl.com/d9vkegg

[19] I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong, "Freenet: A distributed anonymous information storage and retrieval system," in *Designing Privacy Enhancing Technologies.* Springer, 2001, pp. 46–66.

[20] C. Zhang, P. Dhungel, D. Wu, Z. Liu, and K. W. Ross, "BitTorrent Darknets," in *INFOCOM*, 2010, pp. 1460–1468.

[21] P. Biddle, P. Engl, M. Peinado, and B. Willman, "The darknet and the future of content distribution," in *Proceedings of the 2002 ACM Workshop on Digital Rights Management*, 2002.

[22] P. K. Gummadi, S. Saroiu, and S. D. Gribble, "A measurement study of Napster and Gnutella as examples of peer-to-peer file sharing systems," *ACM SIGCOMM Computer Communication Review*, vol. 32, no. 1, pp. 82–82, 2002.

[23] Team Cymru, Inc., "Team Cymru Community Services: The Darknet Project," http://www.team-cymru.org/Services/darknets.html, last accessed in October 2015.

[24] W. Harrop and G. Armitage, "Defining and evaluating greynets (sparse darknets)," in *the IEEE Conference on Local Computer Networks.* IEEE, 2005, pp. 344–350.

[25] N. Provos, "A virtual honeypot framework." in *USENIX Security Symposium*, vol. 173, 2004.

[26] LaBrea: Sticky Honeypot and IDS. http://labrea.sourceforge.net/labrea-info.html. Last accessed in October 2015.

[27] Z. Durumeric, M. Bailey, and J. A. Halderman, "An internet-wide view of internet-wide scanning," in *USENIX Security Symposium*, 2014.

[28] A. Dainotti, A. King, k. Claffy, F. Papale, and A. Pescape, "Analysis of a /0 stealth scan from a botnet," in *Proceedings of the 2012 ACM conference on Internet measurement conference (IMC)*. Boston Massachusetts USA: ACM, 2012, pp. 1–14.

[29] E. Cooke, M. Bailey, F. Jahanian, and R. Mortier, "The dark oracle: Perspective-aware unused and unreachable address discovery," in *NSDI, USENIX*, vol. 6, 2006, pp. 8–8.

[30] D. Moore, G. Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity," in *USENIX Security Symposium*, Washington, D.C., Aug 2001.

[31] C. Fachkha, E. Bou-Harb, and M. Debbabi, "Fingerprinting Internet DNS Amplification DDoS activities," in *6th International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, 2014, pp. 1–5.

[32] C. Rossow, "Amplification hell: Revisiting network protocols for DDoS abuse," in *Symposium on Network and Distributed System Security (NDSS)*, 2014.

[33] M. Kührer, T. Hupperich, C. Rossow, and T. Holz, "Exit from Hell? Reducing the Impact of Amplification DDoS Attacks," in *23rd USENIX Security Symposium (USENIX Security 14)*. San Diego, CA: USENIX Association, Aug. 2014, pp. 111–125. [Online]. Available: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/kuhrer

[34] P. Ferguson and D. Senie, "Network ingress filtering," 2000.

[35] J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang, "Save: Source address validity enforcement protocol," in *Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, vol. 3. IEEE, 2002, pp. 1557–1566.

[36] R. Stewart, "Stream control transmission protocol," *Internet Engineering Task Force*, 2007.

[37] E. P. Rathgeb, C. Hohendorf, and M. Nordhoff, "On the robustness of sctp against dos attacks," in *Third International Conference on Convergence and Hybrid Information Technology (ICCIT)*, vol. 2. IEEE, 2008, pp. 1144–1149.

[38] S. Floyd, M. Handley, and E. Kohler, "Datagram congestion control protocol (dccp)," *Internet Engineering Task Force*, 2006.

[39] Arbor Networks, "Arbor Cloud DDoS Protection Service for Enterprises," http://tinyurl.com/olvcob6, Last accessed in July 2015.

[40] CloudFlare, "The DDoS That Almost Broke the Internet," http://tinyurl.com/c58fbem, last accessed in July 2015.

[41] Sourcefire. A free lightweight network intrusion detection system. [Online]. Available: http://www.snort.org/

[42] Yao *et al.*, "Passive IP traceback: capturing the origin of anonymous traffic through network telescopes," *SIGCOMM Computer Communication*, vol. 41, no. 4, Aug. 2010.

[43] S. M. Bellovin, "Packets Found on an Internet," *Computer Communications Review*, vol. 23, pp. 26–31, 1993.

[44] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "The Spread of the Sapphire/Slammer Worm," CAIDA, ICSI, Silicon Defense, UC Berkeley EECS and UC San Diego CSE, Tech. Rep., 2003.

[45] C. Shannon and D. Moore, "The spread of the witty worm," *IEEE Security & Privacy*, vol. 2, no. 4, pp. 46–50, 2004.

[46] M. Bailey, E. Cooke, F. Jahanian, D. Watson, and J. Nazario, “The blaster worm: Then and now,” *IEEE Security and Privacy*, vol. 3, no. 4, pp. 26–31, Jul. 2005. [Online]. Available: http://dx.doi.org/10.1109/MSP.2005.106

[47] K. Limthong, F. Kensuke, and P. Watanapongse, “Wavelet-based unwanted traffic time series analysis,” in *IEEE International Conference on Computer and Electrical Engineering (ICCEE)*, 2008, pp. 445–449.

[48] Y. Jin, Z.-L. Zhang, K. Xu, F. Cao, and S. Sahu, “Identifying and tracking suspicious activities through IP gray space analysis,” in *Proceedings of the 3rd annual ACM workshop on Mining network data.* ACM, 2007, pp. 7–12.

[49] Y. Jin, G. Simon, K. Xu, Z.-L. Zhang, and V. Kumar, “Grays anatomy: Dissecting scanning activities using IP gray space analysis,” *SysML07*, 2007.

[50] N. Jiang, Y. Jin, A. Skudlark, and Z.-L. Zhang, “Greystar: Fast and accurate detection of SMS spam numbers in large cellular networks using gray phone space,” in *Proceedings of 22nd USENIX Security Symposium*, 2013, pp. 1–16.

[51] V. Yegneswaran, P. Barford, and S. Jha, “Global intrusion detection in the domino overlay system.” in *NDSS*, 2004.

[52] V. Yegneswaran, P. Barford, and D. Plonka, “On the Design and Use of Internet Sinks for Network Abuse Monitoring,” in *proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID)*, 2004, pp. 146–165.

[53] V. Yegneswaran, P. Barford, and V. Paxson, “Using honeynets for internet situational awareness,” in *Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets)*, 2005.

[54] S.-S. Choi, J. Song, S. Kim, and S. Kim, “A model of analyzing cyber threats trend and tracing potential attackers based on darknet traffic,” *Security and Communication Networks*, 2013.

[55] B. Krishnamurthy, “Mohonk: mobile honeypots to trace unwanted traffic early,” in *Proceedings of the ACM SIGCOMM workshop on Network troubleshooting: research, theory and operations practice meet malfunctioning reality*. ACM, 2004, pp. 277–282.

[56] Michael Bailey et al., “A hybrid honeypot architecture for scalable network monitoring,” *Technical Report CSE-TR-499-04, University of Michigan*, 2004.

[57] M. Bailey, E. Cooke, F. Jahanian, N. Provos, K. Rosaen, and D. Watson, “Data reduction for the scalable automated analysis of distributed darknet traffic,” in *Proceedings of the USENIX/ACM Internet Measurement Conference (IMC)*, 2005.

[58] F. Pouget and T. Holz, “A pointillist approach for comparing honeypots,” in *Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, Vienna, AUSTRIA, 07 2005. [Online]. Available: http://www.eurecom.fr/publication/1625

[59] M. Dacier, C. Leita, O. Thonnard, H. Van Pham, and E. Kirda, “Assessing cybercrime through the eyes of the WOMBAT,” in *Cyber Situational Awareness*. Springer, 2010, pp. 103–136.

[60] F. Pouget, M. Dacier, and V. H. Pham, “Leurre.com: on the advantages of deploying a large scale distributed honeypot platform,” in *E-Crime and Computer Conference (ECCE)*. Citeseer, 2005.

[61] P. Komisarczuk and I. Welch, "Internet sensor grid: experiences with passive and active instruments," in *Communications: Wireless in Developing Countries and Networks of the Future.* Springer, 2010, pp. 132–145.

[62] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson, "The Internet Motion Sensor: A Distributed Blackhole Monitoring System," in *proceedings of Network and Distributed System Security Symposium (NDSS*, San Diego, CA, 2005, pp. 1–13.

[63] P.-T. Chen, C.-S. Laih, F. Pouget, and M. Dacier, "Comparative survey of local honeypot sensors to assist network forensics," in *First International Workshop on Systematic Approaches to Digital Forensic Engineering.* IEEE, 2005, pp. 120–132.

[64] R. Berthier and M. Cukier, "The deployment of a darknet on an organization-wide network: An empirical analysis," in *High Assurance Systems Engineering Symposium (HASE).* IEEE, 2008, pp. 59–68.

[65] M. A. Rajab, F. Monrose, and A. Terzis, "On the effectiveness of distributed worm monitoring," in *Proceedings of the 14th USENIX Security Symposium*, 2005, pp. 225–237. [Online]. Available: http://www.usenix.org/event/sec05/tech/full_papers/rajab/rajab_html/

[66] Barford et al., "Toward a model for source addresses of Internet background radiation," in *Proceeding of the Passive and Active Measurement Conference*, 2006.

[67] D. Pemberton, P. Komisarczuk, and I. Welch, "Internet background radiation arrival density and network telescope sampling strategies," in *Australasian Telecommunication Networks and Applications Conference (ATNAC).* IEEE, 2007, pp. 246–252.

[68] M. A. Rajab, F. Monrose, and A. Terzis, “Fast and evasive attacks: Highlighting the challenges ahead,” in *Recent Advances in Intrusion Detection*. Springer, 2006, pp. 206–225.

[69] S. Sinha, M. Bailey, and F. Jahanian, “Shedding light on the configuration of dark addresses.” in *NDSS*, 2007.

[70] Y. Shinoda, K. Ikai, and M. Itoh, “Vulnerabilities of passive internet threat monitors,” in *Proceedings of the 14th USENIX Security Symposium*, 2005, pp. 209–224. [Online]. Available: http://www.usenix.org/event/sec05/tech/full_papers/shinoda/shinoda_html/

[71] J. Bethencourt, J. Franklin, and M. Vernon, “Mapping internet sensors with probe response attacks,” in *USENIX Security*, 2005.

[72] E. Cooke, A. Myrick, D. Rusek, and F. Jahanian, “Resource-aware multi-format network security data storage,” in *Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense.* ACM, 2006, pp. 177–184.

[73] A. Nottingham and B. Irwin, “Towards a GPU accelerated virtual machine for massively parallel packet classification and filtering,” in *Proceedings of the South African Institute for Computer Scientists and Information Technologists Conference.* ACM, 2013, pp. 27–36.

[74] S. Zanero, “Observing the tidal waves of malware: experiences from the WOMBAT project,” in *Proceedings of the 2010 Second Vaagdevi International Conference on Information Technology for Real World Problems.* IEEE Computer Society, 2010, pp. 30–35.

[75] D. Moore, C. Shannon, G. M. Voelker, and S. Savage, *Network telescopes: Technical report.* Department of Computer Science and Engineering, University of California, San Diego, 2004.

[76] CAIDA, "The UCSD Network Telescope," http://www.caida.org/projects/network_telescope/, last accessed in October 2015.

[77] D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, and K. Nakao, "Nicter: An incident analysis system toward binding network monitoring with malware analysis," in *WOMBAT Workshop on Information Security Threats Data Collection and Sharing (WISTDCS)*. IEEE, 2008, pp. 58–66.

[78] M. Eto, D. Inoue, J. Song, J. Nakazato, K. Ohtaka, and K. Nakao, "NICTER: a Large-Scale Network Incident Analysis System: Case Studies for Understanding Threat Landscape," in *proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security*, ser. BADGERS, New York, NY, USA, 2011, pp. 37–45.

[79] C. Leita, V.-H. Pham, O. Thonnard, E. Ramirez, F. Pouget, E. Kirda, and M. Dacier, "The Leurre.com Project: Collecting Internet Threats Information using a Worldwide Distributed Honeynet," in *Proceedings of the 1st WOMBAT Workshop on Information Security Threat Data Exchange (WISTDE)*, 2008, pp. 40–57.

[80] F. Pouget, M. Dacier, H. Debar, and V. H. Pham, "Honeynets: Foundations for the development of early warning information systems," in *Cyberspace Security and Defense: Research Issues*. Springer, 2005, pp. 231–257.

[81] J. Riordan, D. Zamboni, and Y. Duponchel, "Building and deploying Billy Goat, a worm-detection system," IBM Zurich Research Laboratory, pp. 1–12, May 2006.

[82] The Honeynet Project. http://project.honeynet.org/. Last accessed in October 2015.

[83] Internet Storm Center. http://isc.sans.org/. Last accessed in October 2015.

[84] M. Bailey, E. Cooke, T. Battles, and D. McPherson, "Tracking global threats with the Internet Motion Sensor," in *32nd Meeting of the North American Network Operators Group*, 2004.

[85] M. Eto, K. Sonoda, D. Inoue, K. Yoshioka, and K. Nakao, "A Proposal of Malware Distinction Method Based on Scan Patterns Using Spectrum Analysis," *Neural Information Processing*, vol. 5864, pp. 565–572, 2009.

[86] Arakis project. http://www.arakis.pl/pl. Last accessed in October 2015.

[87] NoAH project. http://www.fp6-noah.org. Last accessed in October 2015.

[88] S. Antonatos, K. Anagnostakis, and E. Markatos, "Honey@home: a new approach to large-scale threat monitoring," in *Proceedings of the ACM workshop on recurring malcode*. ACM, 2007, pp. 38–45.

[89] SWITCH Internet Background Noise (IBN). https://www.switch.ch/security/info/ibn/. Last accessed in October 2015.

[90] Police Internet Activities Monitored. http://www.cyberpolice.go.jp/english/obs_e.html. Last accessed in October 2015.

[91] Japan CERT Coordination Center. http://www.jpcert.or.jp/. Last accessed in October 2015.

[92] The IUCC/IDC Internet Telescope. http://noc.ilan.net.il/research/telescope/. Last accessed in October 2015.

[93] RTI, "The Protected Repository for the Defense of Infrastructure Against Cyber Threats," https://www.predict.org, last accessed in October 2015.

[94] T. Zseby *et al.*, “Workshop report: darkspace and unsolicited traffic analysis (DUST 2012),” *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 5, pp. 49–53, 2012.

[95] P. M. Comparetti, G. Salvaneschi, E. Kirda, C. Kolbitsch, C. Kruegel, and S. Zanero, “Identifying dormant functionality in malware programs,” in *IEEE Symposium on Security and Privacy (SP).* IEEE, 2010, pp. 61–76.

[96] C. Leita, M. Dacier, and G. Wicherski, “SGNET: a distributed infrastructure to handle zero-day exploits,” Eurecom, Tech. Rep., 2007. [Online]. Available: http://www.eurecom.fr/publication/2164

[97] G. Portokalidis, A. Slowinska, and H. Bos, “Argos: an emulator for fingerprinting zero-day attacks for advertised honeypots with automatic signature generation,” in *proceedings of EuroSys*, 2006, pp. 15–27.

[98] Paul Baecher and Markus Koetter and Maximillian Dornseif and Felix Freiling, “The Nepenthes Platform: An Efficient Approach to Collect Malware,” in *Proceedings of the 9th International Symposium on Recent Advances in Intrusion Detection (RAID)*, 2006, pp. 165–184.

[99] Van Horenbeeck, M., “The SANS Internet Storm Center,” in *proceedings of WOMBAT Workshop on Information Security Threats Data Collection and Sharing (WISTDCS)*, 2008, pp. 17–23.

[100] DShield: Community-based collaborative firewall log correlation system. http://www.dshield.org/. Last accessed in October 2015.

[101] D. Inoue, M. Suzuki, M. Eto, K. Yoshioka, and K. Nakao, “DAEDALUS: Novel Application of Large-Scale Darknet Monitoring for Practical Protection of Live Networks,” in *Recent Advances in Intrusion Detection.* Springer, 2009, pp. 381–382.

[102] Research and Education Networking Information Sharing and Analysis Center. http://www.ren-isac.net/. Last accessed in October 2015.

[103] An introduction to the simwood darknet. http://blog.simwood.com/2011/08/an-introduction-to-the-simwood-darknet/. Last accessed in October 2015.

[104] The darknet mesh project. http://projects.oucs.ox.ac.uk/darknet/. Last accessed in October 2015.

[105] Irwin, Barry and Vivian William, "A framework for the application of network telescope sensors in a global IP network," Ph.D. dissertation, Rhodes University, 2011.

[106] B. Irwin, "A baseline study of potentially malicious activity across five network telescopes," in *5th International Conference on Cyber Conflict (CyCon)*, 2013, pp. 1–17.

[107] M. Ford, J. Stevens, and J. Ronan, "Initial Results from an IPv6 Darknet," in *Proceedings of the IEEE International Conference on Internet Surveillance and Protection (ICISP)*, 2006, pp. 13–. [Online]. Available: http://dx.doi.org/10.1109/ICISP.2006.14

[108] R. Pang, V. Yegneswaran, P. Barford, V. Paxson, and L. Peterson, "Characteristics of Internet background radiation," in *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*. ACM, 2004, pp. 27–40.

[109] A. SHIMODA, T. MORI, and S. Goto, "Extended Darknet: Multi-Dimensional Internet Threat Monitoring System," *IEICE Transactions on Communications*, pp. 1915–1923, 2012.

[110] A. Dainotti, K. Benson, A. King, M. Kallitsis, E. Glatz, X. Dimitropoulos *et al.*, "Estimating Internet address space usage through passive measurements," *ACM SIGCOMM Computer Communication Review*, pp. 42–49, 2013.

[111] K. Fukuda, T. Hirotsu, O. Akashi, and T. Sugawara, "Correlation among piecewise unwanted traffic time series," in *Global Telecommunications Conference, IEEE GLOBECOM*, 2008, pp. 1–5.

[112] K. Fukuda, H. Toshio, O. Akashi, and T. Sugawara, "A PCA analysis of daily unwanted traffic," in *24th IEEE International Conference on Advanced Information Networking and Applications (AINA)*, 2010, pp. 377–384.

[113] J. Oberheide, M. Karir, and Z. M. Mao, "Characterizing dark DNS behavior," in *Fourth GI International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 07)*, 2007, pp. 140–156.

[114] J. Czyz, K. Lady, S. G. Miller, M. Bailey, M. Kallitsis, and M. Karir, "Understanding IPv6 Internet background radiation," in *Internet Measurement Conference (IMC)*, 2013, pp. 105–118.

[115] E. Glatz and X. Dimitropoulos, "Classifying Internet one-way traffic," in *Proceedings of the 12th ACM SIGMETRICS/PERFORMANCE joint international conference on Measurement and Modeling of Computer Systems*, 2012, pp. 417–418. [Online]. Available: http://doi.acm.org/10.1145/2254756.2254821

[116] R. Wang, L. Zhang, and Z. Liu, "A novel method of filtering internet background radiation traffic," in *Fourth International Conference on Emerging Intelligent Data and Web Technologies (EIDWT)*, 2013, pp. 371–376.

[117] B. Cowie and B. Irwin, "Data classification for artificial intelligence construct training to aid in network incident identification using network telescope data," in *Proceedings of the Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists (SAICSIT)*, 2010, pp. 356–360.

[118] Y. Peng, J. Gong, W. Yang, and W. Liu, "Disclosing the element distribution of bloom filter," in *Computational Science–ICCS 2006*. Springer, 2006, pp. 1022–1025.

[119] H. Rahmani, N. Sahli, and F. Kammoun, "Joint entropy analysis model for ddos attack detection," in *IEEE Fifth International Conference on Information Assurance and Security (IAS)*, vol. 2, 2009, pp. 267–271.

[120] Z. M. Fadlullah, T. Taleb, A. V. Vasilakos, M. Guizani, and N. Kato, "DTRAB: combating against attacks on encrypted protocols through traffic-feature analysis," *IEEE/ACM Transactions on Networking (TON)*, pp. 1234–1247, 2010.

[121] Ł. Saganowski, T. Andrysiak, M. Choraś, and R. Renk, "Expansion of Matching Pursuit Methodology for Anomaly Detection in Computer Networks," in *Computer Recognition Systems 4*. Springer, 2011, pp. 727–736.

[122] M. Choras, L. Saganowski, R. Renk, and W. Holubowicz, "Statistical and signal-based network traffic recognition for anomaly detection," *Expert Systems*, pp. 232–245, 2012.

[123] P. Chhabra, A. John, and H. Saran, "PISA: Automatic Extraction of Traffic Signatures," in *Fourth International Conference in Networking*, 2005, pp. 730–742.

[124] X. He and S. Parameswaran, "MCAD: Multiple connection based anomaly detection," in *11th IEEE Singapore International Conference on Communication Systems (ICCS)*, 2008, pp. 999–1004.

[125] K. Dassouki, H. Debar, H. Safa, and A. Hijazi, “A TCP delay-based mechanism for detecting congestion in the Internet,” in *Third International Conference on Communications and Information Technology (ICCIT)*. IEEE, 2013, pp. 141–145.

[126] C. Labovitz, A. Ahuja, and M. Bailey, “Shining light on dark address space,” Arbor Netwoks, Ann Arbor, Michigan, USA, Tech. Rep. TR-2001-01, November 2001.

[127] J. Francois, O. Festor *et al.*, “Tracking global wide configuration errors,” in *IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation*, 2006.

[128] U. Harder, M. W. Johnson, J. T. Bradley, and W. J. Knottenbelt, “Observing Internet worm and virus attacks with a small network telescope,” *Electronic Notes in Theoretical Computer Science*, pp. 47–59, 2006.

[129] T. Holz, “Learning More About Attack Patterns With Honeypots,” in *Proceedings of Sicherheit*, 2006, pp. 30–41.

[130] J. François, R. State, and O. Festor, “Activity Monitoring for large honeynets and network telescopes,” *International Journal On Advances in Systems and Measurements*, vol. 1, no. 1, pp. 1–13, 2008.

[131] M. OHTA, S. SUGIMOTO, K. FUKUDA, T. HIROTSU, O. AKASHI, and T. SUGAWARA, “Analysis of time-series correlations of packet arrivals to darknet and their size- and location-dependencies,” *Computer Software*, vol. 28, no. 2, 2011.

[132] D. Inoue, K. Yoshioka, M. Eto, Y. Hoshizawa, and K. Nakao, “Malware behavior analysis in isolated miniature network for revealing malware’s network activity,” in *IEEE International Conference on Communications (ICC)*, 2008, pp. 1715–1721.

[133] R. Berthier, D. Korman, M. Cukier, M. Hiltunen, G. Vesonder, and D. Sheleheda, “On the comparison of network attack datasets: An empirical analysis,” in *11th IEEE High Assurance Systems Engineering Symposium (HASE)*, 2008, pp. 39–48.

[134] V. Yegneswaran, P. Barford, and J. Ullrich, “Internet intrusions: Global characteristics and prevalence,” in *ACM SIGMETRICS Performance Evaluation Review*, 2003, pp. 138–147.

[135] R. Rangadurai Karthick, V. Hattiwale, and B. Ravindran, “Adaptive network intrusion detection system using a hybrid approach,” in *Fourth International Conference on Communication Systems and Networks (COMSNETS)*, 2012, pp. 1–7.

[136] P. Barford, Y. Chen, A. Goyal, Z. Li, V. Paxson, and V. Yegneswaran, “Employing honeynets for network situational awareness,” in *Cyber Situational Awareness*, ser. Advances in Information Security, 2010, vol. 46, pp. 71–102.

[137] D. Inoue, K. Yoshioka, M. Eto, M. Yamagata, E. Nishino, J. Takeuchi, K. Ohkouchi, and K. Nakao, “An incident analysis system nicter and its analysis engines based on data mining techniques,” in *Advances in Neuro-Information Processing*. Springer, 2009, pp. 579–586.

[138] O. Thonnard and M. Dacier, “Actionable knowledge discovery for threats intelligence support using a multi-dimensional data mining methodology,” in *IEEE International Conference on Data Mining Workshops (ICDMW)*, 2008, pp. 154–163.

[139] O. Thonnard and D. Marc, “A framework for attack patterns’ discovery in honeynet data,” *Digital Investigation*, vol. 5, Supplement, pp. S128 – S139, 2008, the Proceedings of the Eighth Annual DFRWS

Conference. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287608000431

[140] O. Thonnard, W. Mees, and M. Dacier, "Addressing the attack attribution problem using knowledge discovery and multi-criteria fuzzy decision-making," in *Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics*, 2009, pp. 11–21. [Online]. Available: http://doi.acm.org/10.1145/1599272.1599277

[141] S. Sinha, M. Bailey, and F. Jahanian, "One size does not fit all: 10 years of applying context-aware security," in *IEEE Conference on Technologies for Homeland Security (HST)*, 2009, pp. 14–21.

[142] C. Fachkha, E. Bou-Harb, A. Boukhtouta, S. Dinh, F. Iqbal, and M. Debbabi, "Investigating the Dark Cyberspace: Profiling, Threat-Based Analysis and Correlation," in *7th International Conference on Risk and Security of Internet and Systems (CRiSIS)*. Cork, Ireland: IEEE, 2012, pp. 1–8.

[143] E. Ahmed, A. Clark, and G. Mohay, "A novel sliding window based change detection algorithm for asymmetric traffic," in *IFIP International Conference on Network and Parallel Computing (NPC)*. IEEE, 2008, pp. 168–175.

[144] E. Ahmed, C. Andrew, and M. George, "Effective change detection in large repositories of unsolicited traffic," *International Conference on Internet Monitoring and Protection*, vol. 0, pp. 1–6, 2009.

[145] W. Chen, Y. Liu, and Y. Guan, "Cardinality change-based early detection of large-scale cyber-attacks," in *Proceedings IEEE INFOCOM*, 2013, pp. 1788–1796.

[146] S. Soltani, S. A. Khayam, and H. Radha, “Detecting malware outbreaks using a statistical model of blackhole traffic,” in *IEEE International Conference on Communications (ICC)*, 2008, pp. 1593–1597.

[147] M. Casado, T. Garfinkel, W. Cui, V. Paxson, and S. Savage, “Opportunistic measurement: Extracting insight from spurious traffic,” in *Proceedings of the 4th ACM Workshop on Hot Topics in Networks (Hotnets-IV)*, 2005.

[148] A. Clark, M. Dacier, G. Mohay, F. Pouget, and J. Zimmermann, “Internet attack knowledge discovery via clusters and cliques of attack traces,” *Journal of Information Assurance and Security*, vol. 1, no. 1, pp. 21–32, 2006. [Online]. Available: http://eprints.qut.edu.au/22973/

[149] S. O. Hunter, B. Irwin, and E. Stalmans, “Real-time distributed malicious traffic monitoring for honeypots and network telescopes,” in *Information Security for South Africa, 2013.* IEEE, 2013, pp. 1–9.

[150] R. Gupta, K. Ramamritham, and M. Mohania, “Ratio threshold queries over distributed data sources,” *Proceedings of the VLDB Endowment*, vol. 6, no. 8, pp. 565–576, 2013.

[151] E. Cooke, Z. M. Mao, and F. Jahanian, “Hotspots: The root causes of non-uniformity in self-propagating malware,” in *IEEE International Conference on Dependable Systems and Networks (DSN)*, 2006, pp. 179–188.

[152] H. Luo, Y. Lin, H. Zhang, and M. Zukerman, “Preventing DDoS attacks by identifier/locator separation,” *IEEE Network*, pp. 60–65, 2013.

[153] M. Callau-Zori, R. Jiménez-Peris, V. Gulisano, M. Papatriantafilou, Z. Fu, and M. Patiño-Martínez, “STONE: a stream-based DDoS defense framework,” in *Proceedings of the 28th Annual ACM Symposium on Applied Computing*, 2013, pp. 807–812.

[154] P. Arun Raj Kumar, and S. Selvakumar, “Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems,” *Computer Communications*, vol. 36, no. 3, pp. 303 – 319, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366412003222

[155] S. Bhatia, D. Schmidt, and G. Mohay, “Ensemble-based ddos detection and mitigation model,” in *Proceedings of the Fifth International Conference on Security of Information and Networks (SIN)*, 2012, pp. 79–86.

[156] S. Bhatia, G. Mohay, A. Tickle, and E. Ahmed, “Parametric differences between a real-world distributed denial-of-service attack and a flash event,” in *Sixth International Conference on Availability, Reliability and Security (ARES)*, 2011, pp. 210–217.

[157] C. Fachkha, E. Bou-Harb, and M. Debbabi, “Towards a Forecasting Model for Distributed Denial of Service Activities,” in *12th IEEE International Symposium on Network Computing and Applications (NCA)*. IEEE, 2013, pp. 110–117.

[158] C. Fachkha, E. Bou Harb, and M. Debbabi, “On the inference and prediction of DDoS campaigns,” *Wireless Communications and Mobile Computing*, 2014. [Online]. Available: http://dx.doi.org/10.1002/wcm.2510

[159] E. Feitosa, E. Souto, and D. H. Sadok, “An orchestration approach for unwanted internet traffic identification,” *Computer Networks*, vol. 56, no. 12, pp. 2805 – 2831, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128612001582

[160] H. Rahmani, N. Sahli, and F. Kamoun, “DDoS flooding attack detection scheme based on F-divergence,” *Computer Communications*,

vol. 35, no. 11, pp. 1380 – 1391, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366412001156

[161] H. Liu, Y. Sun, V. Valgenti, and M. S. Kim, "Trustguard: A flow-level reputation-based ddos defense system," in *Consumer Communications and Networking Conference (CCNC), IEEE*, 2011, pp. 287–291.

[162] E. Ahmed, G. Mohay, A. Tickle, and S. Bhatia, "Use of IP Addresses for High Rate Flooding Attack Detection," in *Security and Privacy Silver Linings in the Cloud*, ser. IFIP Advances in Information and Communication Technology, 2010, vol. 330, pp. 124–135.

[163] D. Moore, C. Shannon *et al.*, "Code-red: a case study on the spread and victims of an internet worm," in *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*. ACM, 2002, pp. 273–284.

[164] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the slammer worm," *IEEE Security & Privacy*, pp. 33–39, 2003.

[165] V. H. Berk, R. S. Gray, and G. Bakos, "Using sensor networks and data fusion for early detection of active worms," in *AeroSense 2003*. International Society for Optics and Photonics, 2003, pp. 92–104.

[166] Staniford *et al.*, "The top speed of flash worms," in *Proceedings of the ACM workshop on Rapid malcode*, ser. WORM '04. New York, NY, USA: ACM, 2004, pp. 33–42.

[167] E. Cooke, Z. M. Mao, and F. Jahanian, "Worm hotspots: Explaining non-uniformity in worm targeting behavior," *University of Michigan TR*, 2004.

[168] D. W. Richardson, S. D. Gribble, and E. D. Lazowska, "The limits of global scanning worm detectors in the presence of background noise," in *Proceedings*

of the ACM workshop on Rapid malcode (WORM), 2005, pp. 60–70. [Online]. Available: http://doi.acm.org/10.1145/1103626.1103638

[169] A. Kumar, V. Paxson, and N. Weaver, "Exploiting underlying structure for detailed reconstruction of an internet-scale event," in *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement (IMC)*. Berkeley, CA, USA: USENIX Association, 2005, pp. 33–33. [Online]. Available: http://dl.acm.org/citation.cfm?id=1251086.1251119

[170] M. Abu Rajab, F. Monrose, and A. Terzis, "Worm evolution tracking via timing analysis," in *Proceedings of the 2005 ACM workshop on Rapid malcode*, ser. WORM '05. New York, NY, USA: ACM, 2005, pp. 52–59. [Online]. Available: http://doi.acm.org/10.1145/1103626.1103637

[171] C. C. Zou, W. Gong, D. Towsley, and L. Gao, "The monitoring and early detection of internet worms," *IEEE/ACM Transactions on Networking (TON)*, vol. 13, no. 5, pp. 961–974, 2005.

[172] V.-H. Pham, M. Dacier, G. Urvoy-Keller, and T. En-Najjary, "The quest for multi-headed worms," in *Proceedings of the 5th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*, 2008, pp. 247–266.

[173] Y. Kanda, K. Fukuda, and T. Sugawara, "A flow analysis for mining traffic anomalies," in *IEEE International Conference on Communications (ICC)*, 2010, pp. 1–5.

[174] Q. Wang, Z. Chen, K. Makki, N. Pissinou, and C. Chen, "Inferring internet worm temporal characteristics," in *GLOBECOM*, 2008, pp. 2007–2012.

[175] Q. Wang, Z. Chen, and C. Chen, “Darknet-based inference of internet worm temporal characteristics,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 4, pp. 1382–93, Dec. 2011.

[176] B. Irwin, “A network telescope perspective of the Conficker outbreak,” in *Information Security for South Africa (ISSA)*, 2012, pp. 1 –8.

[177] Z. Chen, C. Lin, J. Ni, D.-H. Ruan, B. Zheng, Y.-X. Jiang, X.-H. Peng, Y. Wang, A.-a. Luo, B. Zhu *et al.*, “AntiWorm NPU-based parallel bloom filters for TCP/IP content processing in Giga-Ethernet LAN,” in *The IEEE Conference on Local Computer Networks*, 2005, pp. 748–755.

[178] C. C. Zou, L. Gao, W. Gong, and D. Towsley, “Monitoring and early warning for internet worms,” in *Proceedings of the 10th ACM conference on Computer and communications security (CCS)*, NY, USA, 2003, pp. 190–199. [Online]. Available: http://doi.acm.org/10.1145/948109.948136

[179] D. Dagon, C. Zou, and W. Lee, “Modeling botnet propagation using time zones,” in *Proceedings of the 13th Network and Distributed System Security Symposium (NDSS)*, San Diego, California USA, 2006.

[180] V.-H. Pham and M. Dacier, “Honeypot traces forensics : the observation view point matters,” Eurecom, Tech. Rep. EURECOM+2697, 2009. [Online]. Available: http://www.eurecom.fr/publication/2697

[181] P. Wang, S. Sparks, and C. C. Zou, “An advanced hybrid peer-to-peer botnet,” *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 2, pp. 113–127, 2010.

[182] E. Cooke, F. Jahanian, and D. McPherson, “The Zombie roundup: understanding, detecting, and disrupting botnets,” in *Proceedings of the Steps to Reducing Unwanted Traffic on the Internet on Steps to*

Reducing Unwanted Traffic on the Internet Workshop (SRUTI). Berkeley, CA, USA: USENIX Association, 2005, pp. 6–6. [Online]. Available: http://dl.acm.org/citation.cfm?id=1251282.1251288

[183] G. Gu, R. Perdisci, J. Zhang, and W. Lee, "Botminer: clustering analysis of network traffic for protocol- and structure-independent botnet detection," in *Proceedings of the 17th conference on Security Symposium (SS)*. Berkeley, CA, USA: USENIX Association, 2008, pp. 139–154. [Online]. Available: http://dl.acm.org/citation.cfm?id=1496711.1496721

[184] A. Ramachandran, N. Feamster, and D. Dagon, "Revealing botnet membership using dnsbl counter-intelligence," *Proc. 2nd USENIX Steps to Reducing Unwanted Traffic on the Internet*, pp. 49–54, 2006.

[185] A. Ramachandran and N. Feamster, "Understanding the network-level behavior of spammers," in *ACM SIGCOMM Computer Communication Review*, vol. 36, no. 4. ACM, 2006, pp. 291–302.

[186] G. Gu, P. A. Porras, V. Yegneswaran, M. W. Fong, and W. Lee, "Bothunter: Detecting malware infection through ids-driven dialog correlation." in *USENIX Security*, vol. 7, 2007, pp. 1–16.

[187] E. Bou-Harb, M. Debbabi, and C. Assi, "A statistical approach for fingerprinting probing activities," in *Eighth International Conference on Availability, Reliability and Security (ARES)*, 2013, pp. 21–30.

[188] B.-H. Elias, D. Mourad, and A. Chadi, "A systematic approach for detecting and clustering distributed cyber scanning," *Computer Networks*, vol. 57, no. 18, pp. 3826 – 3839, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128613003137

[189] Z. Li, A. Goyal, Y. Chen, and V. Paxson, "Automating analysis of large-scale botnet probing events," in *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, 2009, pp. 11–22.

[190] A. Dainotti, A. King, and K. Claffy, "Analysis of Internet-wide Probing using Darknets," in *Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*, 2012.

[191] G. Gu, Z. Chen, P. Porras, and W. Lee, "Misleading and defeating importance-scanning malware propagation," in *Third International Conference on Security and Privacy in Communications Networks. SecureComm*, 2007, pp. 250–259.

[192] Z. Li, A. Goyal, and Y. Chen, "Honeynet-based botnet scan traffic analysis," in *Botnet Detection*. Springer, 2008, pp. 25–44.

[193] M. Eto, D. Inoue, M. Suzuki, and K. Nakao, "A Statistical Packet Inspection for Extraction of Spoofed IP Packets on Darknet," in *Proceedings of the Joint Workshop on Information Security, Kaohsiung, Taiwan*, 2009.

[194] M. Ohta, Y. Kanda, K. Fukuda, and T. Sugawara, "Analysis of Spoofed IP Traffic Using Time-to-Live and Identification Fields in IP Headers," in *IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA)*, 2011, pp. 355 –361.

[195] J. Bi, P. Hu, and P. Li, "Study on Classification and Characteristics of Source Address Spoofing Attacks in the Internet," in *Proceedings of the Ninth International Conference on Networks (ICN)*. Washington, DC, USA: IEEE Computer Society, 2010, pp. 226–230.

[196] A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, and A. Pescapé, "Analysis of country-wide internet outages caused by censorship,"

in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference.* ACM, 2011, pp. 1–18.

[197] M. Bailey and C. Labovitz, "Censorship and Co-option of the Internet Infrastructure," University of Michigan, Ann Arbor, MI, USA, Tech. Rep. CSE-TR-572-11, July 2011.

[198] K. Benson, A. Dainotti, K. Claffy, and E. Aben, "Gaining insight into as-level outages through analysis of internet background radiation," in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2013, pp. 447–452.

[199] L. Quan, J. Heidemann, and Y. Pradkin, "Trinocular: understanding Internet reliability through adaptive probing," in *Proceedings of the ACM SIGCOMM conference on SIGCOMM.* ACM, 2013, pp. 255–266.

[200] J. Riihijarvi, P. Mahonen, and M. Wellens, "Metrics for characterizing complexity of network traffic," in *IEEE International Conference on Telecommunications (ICT)*, 2008, pp. 1–6.

[201] J. Riihijarvi, M. Wellens, and P. Mahonen, "Measuring complexity and predictability in networks with multiscale entropy analysis," in *IEEE INFOCOM*, 2009, pp. 1107–1115.

[202] Mallat, Stéphane G and Zhang, Zhifeng, "Matching pursuits with time-frequency dictionaries," *IEEE Transactions on Signal Processing*, vol. 41, no. 12, pp. 3397–3415, 1993.

[203] Corrado Leita and Ken Mermoud and Marc Dacier, "ScriptGen: an Automated Script Generation Tool for honeyd," in *proceedings of ACSAC*, 2005, pp. 203–214.

[204] N. Abouzakhar and A. Bakar, "A chi-square testing-based intrusion detection model," in *Proceedings of the 4th International Conference on Cybercrime Forensics Education & Training*, 2010.

[205] N. Abouzakhar, H. Chen, and B. Christianson, "An Enhanced Fuzzy ARM Approach for Intrusion Detection," *IJDCF*, pp. 41–61, 2011.

[206] T. Andrysiak, Ł. Saganowski, and M. Choraś, "DDoS Attacks Detection by Means of Greedy Algorithms," in *Image Processing and Communications Challenges*. Springer, 2013, pp. 303–310.

[207] MAWI Working Group Traffic Archive. http://mawi.wide.ad.jp/mawi/. Last accessed in October 2015.

[208] CERT advisory, "Smurf IP Denial-of-Service Attacks," http://www.cert.org/historical/advisories/CA-1998-01.cfm?, last accessed in October 2015.

[209] V. Paxson, "An Analysis of Using Reflectors for Distributed Denial-of-service Attacks," *SIGCOMM Comput. Commun. Rev.*, vol. 31, no. 3, pp. 38–47, Jul. 2001. [Online]. Available: http://doi.acm.org/10.1145/505659.505664

[210] M. Kührer, T. Hupperich, C. Rossow, and T. Holz, "Hell of a handshake: abusing TCP for reflective amplification DDoS attacks," in *USENIX Workshop on Offensive Technologies (WOOT)*, 2014.

[211] CloudFlare blog. The DDoS That Knocked Spamhaus Offline. Last accessed in October 2015. [Online]. Available: http://tinyurl.com/d46gpkj

[212] E. Bou-Harb, C. Fachkha, M. Debbabi, and C. Assi, "Inferring internet-scale infections by correlating malware and probing activities," in *IEEE International Conference on Communications (ICC)*. IEEE, 2014, pp. 640–646.

[213] D. Q. Le, T. Jeong, H. E. Roman, and J. W.-K. Hong, "Traffic dispersion graph based anomaly detection," in *Proceedings of the Second*

Symposium on Information and Communication Technology, ser. SoICT. New York, NY, USA: ACM, 2011, pp. 36–41. [Online]. Available: http://doi.acm.org/10.1145/2069216.2069227

[214] C. Joslyn, S. Choudhury, D. Haglin, B. Howe, B. Nickless, and B. Olsen, "Massive scale cyber traffic analysis: a driver for graph database research," in *First International Workshop on Graph Data Management Experiences and Systems*. ACM, 2013, p. 3.

[215] Krasser et al., "Real-time and forensic network data analysis using animated and coordinated visualization," in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop (IAW)*, 2005, pp. 42–49.

[216] J.-P. van Riel and B. Irwin, "InetVis, a visual tool for network telescope traffic analysis," in *Proceedings of the 4th international conference on Computer graphics, virtual reality, visualisation and interaction in Africa*. ACM, 2006, pp. 85–89.

[217] B. Irwin and J.-P. van Riel, "Using inetvis to evaluate snort and bro scan detection on a network telescope," in *VizSEC 2007*. Springer, 2008, pp. 255–273.

[218] Harrop et al., "Real-time collaborative network monitoring and control using 3d game engines for representation and interaction," in *Proceedings of the 3rd international workshop on Visualization for computer security (VizSEC)*. ACM, 2006, pp. 31–40. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179583

[219] W. Harrop and G. Armitage, "Modifying first person shooter games to perform real time network monitoring and control tasks," in *Proceedings of 5th ACM SIGCOMM workshop on Network and system support for*

games (NetGames). New York, NY, USA: ACM, 2006. [Online]. Available: http://doi.acm.org/10.1145/1230040.1230074

[220] L. Parry, "L3dgeworld 2.3 input and output specifications," *Centre for Advanced Internet Architectures, Swinburne University of Technology*, vol. 80222, p. 22, 2008.

[221] K. Fukuda and R. Fontugne, "Estimating speed of scanning activities with a hough transform," in *IEEE International Conference on Communications (ICC)*, ser. IEEE International Conference on Communications, 2010.

[222] R. Fontugne, T. Hirotsu, and K. Fukuda, "An image processing approach to traffic anomaly detection," in *Proceedings of the 4th Asian Conference on Internet Engineering*. ACM, 2008, pp. 17–26.

[223] Fontugne et al., "A visualization tool for exploring multi-scale network traffic anomalies," in *IEEE International Symposium on Performance Evaluation of Computer & Telecommunication Systems (SPECTS)*, vol. 41, 2009, pp. 274–281.

[224] H. Choi, H. Lee, and H. Kim, "Fast detection and visualization of network attacks on parallel coordinates," *Computers and Security*, vol. 28, no. 5, pp. 276 – 288, 2009.

[225] B. Irwin and N. Pilkington, "High level Internet scale traffic visualization using hilbert curve mapping," in *VizSEC 2007*. Springer, 2008, pp. 147–158.

[226] CAIDA. Caida visualization toolsl. https://www.caida.org/tools/visualization/. Last accessed in September 2015.

[227] L. Spitzner, "Honeytokens: The other honeypot," 2003.

[228] D. Whyte, P. C. van Oorschot, and E. Kranakis, "Tracking darkports for network defense." in *ACSAC*, 2007, pp. 161–171.

[229] Garcia-Teodoro et al., “Anomaly-based network intrusion detection: Techniques, systems and challenges,” *Computers & Security*, vol. 28, no. 1, pp. 18–28, 2009.

[230] T. Peng, C. Leckie, and K. Ramamohanarao, “Survey of network-based defense mechanisms countering the DoS and DDoS problems,” *ACM Computing Surveys*, vol. 39, no. 1, Apr. 2007.

[231] Z. Zhu, G. Lu, Y. Chen, Z. Fu, P. Roberts, and K. Han, “Botnet research survey,” in *32nd Annual IEEE International Computer Software and Applications (COMPSAC)*, 2008, pp. 967–972.

[232] M. Bailey, E. Cooke, F. Jahanian, Y. Xu, and M. Karir, “A survey of botnet technology and defenses,” in *Proceedings of the Cybersecurity Applications & Technology Conference for Homeland Security (CATCH)*, Washington, USA, 2009, pp. 299–304.

[233] P. Li, M. Salour, and X. Su, “A survey of Internet worm detection and containment,” *IEEE Communications Surveys Tutorials*, vol. 10, no. 1, pp. 20 –35, 2008.

[234] M. H. Bhuyan, D. Bhattacharyya, and J. Kalita, “Surveying port scans and their detection methodologies,” *The Computer Journal*, 2011. [Online]. Available: http://comjnl.oxfordjournals.org/content/early/2011/04/19/comjnl.bxr035.abstract

[235] F. Zhang, S. Zhou, Z. Qin, and J. Liu, “Honeypot: a supplemented active defense system for network security,” in *The Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*. IEEE, 2003, pp. 231–235.

[236] C. Seifert, I. Welch, and P. Komisarczuk, "Taxonomy of honeypots, july 2006 2006," 2006.

[237] H. F. Matthew L. Bringer, Christopher A. Chelmecki, "A survey: Recent advances and future trends in honeypot research," *International Journal of Computer Network and Information Security (IJCNIS)*, 2012.

[238] E. Bou-Harb, M. Debbabi, and C. Assi, "Cyber Scanning: A Comprehensive Survey," *Communications Surveys Tutorials, IEEE*, vol. 16, no. 3, pp. 1496–1519, March 2014.

[239] NMAP, "Port Scanning Techniques," http://nmap.org/book/man-port-scanning-techniques.html, last accessed in October 2015.

[240] CAIDA, "Conficker/Conflicker/Downadup as seen from the UCSD Network Telescope," http://www.caida.org/research/security/ms08-067/conficker.xml, last accessed in March 2015.

[241] Y. Yao, W. long Xiang, H. Guo, G. Yu, and F.-X. Gao, "Diurnal forced models for worm propagation based on conficker dataset," in *Third International Conference on Multimedia Information Networking and Security (MINES)*, Nov 2011, pp. 431–435.

[242] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir, "Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks," in *Proceedings of the 2014 Conference on Internet Measurement Conference*. ACM, 2014, pp. 435–448.

[243] C. Fachkha, E. Bou-Harb, and M. Debbabi, "Inferring Distributed Reflection Denial of Service Attacks from Darknet," *Computer Communications*, 2015.

[244] D. Sisalem, J. Kuthan, and S. Ehlert, "Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms," *Network, IEEE*, vol. 20, no. 5, pp. 26 –31, September-October 2006.

[245] APWG, "Global phishing survey: Trends and domain name use in 2h2011." [Online]. Available: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2011.pdf

[246] M. S. TechCenter, "Microsoft security bulletin ms09-018 - critical," Available at: http://technet.microsoft.com/en-us/security/bulletin/MS09-018.

[247] S. Shah, "Top ten web attacks," Available at: http://www.blackhat.com/presentations/bh-asia-02/bh-asia-02-shah.pdf.

[248] L. S. Online, "MS terminal service cracking," Available at: http://www.carnal0wnage.com/papers/lso_ms_terminal_server_cracking.pdf.

[249] V. Paxson, "Bro: a system for detecting network intruders in real-time," *Computer networks*, vol. 31, no. 23, pp. 2435–2463, 1999.

[250] A. Thomas, "Rapid: Reputation based approach for improving intrusion detection effectiveness," in *Sixth International Conference on Information Assurance and Security (IAS)*, August 2010, pp. 118 –124.

[251] National Institute of Standards and Technology (NIST)-National Cyber-Alert System, "Vulnerability summary for cve-2007-2931," 2011, Available at: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-2931.

[252] R. Agrawal, T. Imielinski, and A. Swami, "Mining association rules between sets of items in large databases," *ACM SIGMOD Record*, vol. 22, no. 2, pp. 207–216, June 1993.

[253] J. Han and J. Pei, "Mining frequent patterns by pattern-growth: methodology and implications," *ACM SIGKDD Explorations Newsletter*, pp. 14–20, December 2000.

[254] M. J. Zaki, "Scalable algorithms for association mining," *IEEE Transactions of Knowledge and Data Engineering (TKDE)*, vol. 12, pp. 372–390, 2000.

[255] J. D. Holt and S. M. Chung, "Efficient mining of association rules in text databases," in *8th ACM International Conference on Information and Knowledge Management (CIKM)*, Kansas City, Missouri, United States, 1999, pp. 234–242.

[256] J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques (The Morgan Kaufmann Series in Data Management Systems)*, 2nd ed. Morgan Kaufmann, January 2006.

[257] Ian H. Witten, Eibe Frank, Mark A. Hall, *Data Mining: Practical Machine Learning Tools and Techniques*, 3rd ed. Morgan Kaufmann, January 2011.

[258] K. Fukuda, L. A. N. Amaral, and H. E. Stanley, "Dynamics of temporal correlation in daily Internet traffic," in *Global Telecommunications Conference. GLOBECOM*, vol. 7. IEEE, 2003, pp. 4069–4073.

[259] M. Allman, V. Paxson, and J. Terrell, "A brief history of scanning," in *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, ser. IMC '07. New York, NY, USA: ACM, 2007, pp. 77–82. [Online]. Available: http://doi.acm.org/10.1145/1298306.1298316

[260] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted Denial of Service Attacks: The Shrew vs. The Mice and Elephants," in *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols*

for Computer Communications (SIGCOMM). New York, NY, USA: ACM, 2003, pp. 75–86.

[261] Z. Li, A. Goyal, Y. Chen, and V. Paxson, "Towards situational awareness of large-scale botnet probing events," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 175–188, 2011.

[262] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," *ACM Transactions on Computer Systems (TOCS)*, vol. 24, no. 2, pp. 115–139, 2006.

[263] J. D. Hamilton, *Time series analysis*. Princeton University Press, 1994, vol. 2.

[264] C.-K. Peng, S. V. Buldyrev, S. Havlin, M. Simons, H. E. Stanley, and A. L. Goldberger, "Mosaic organization of dna nucleotides," *Physical Review E*, vol. 49, no. 2, p. 1685, 1994.

[265] M. B. Priestley, *Spectral analysis and time series*. Academic press, 1981.

[266] J. A. Matos, S. Gama, H. J. Ruskin, A. A. Sharkasi, and M. Crane, "Time and scale Hurst exponent analysis for financial markets," *Physica A: Statistical Mechanics and its Applications*, vol. 387, no. 15, pp. 3910–3915, 2008.

[267] Hu, Kun and Ivanov, Plamen Ch and Chen, Zhi and Carpena, Pedro and Stanley, H Eugene, "Effect of trends on detrended fluctuation analysis," *Physical Review E*, vol. 64, no. 1, p. 011114, 2001.

[268] B. Zhou, D. He, Z. Sun, and W. H. Ng, "Network traffic modeling and prediction with arima/garch," in *Proc. of HET-NETs Conference*. Citeseer, 2005, pp. 1–10.

[269] Y. Zhuang, L. Chen, X. S. Wang, and J. Lian, "A weighted moving average-based approach for cleaning sensor data," in *27th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2007, pp. 38–38.

[270] M. Papadopouli, E. Raftopoulos, and H. Shen, “Evaluation of short-term traffic forecasting algorithms in wireless networks,” in *2nd Conference on Next Generation Internet Design and Engineering (NGI)*. Valencia, Spain: IEEE, 2006, pp. 8–pp.

[271] A. Goia, C. May, and G. Fusai, “Functional clustering and linear regression for peak load forecasting,” *International Journal of Forecasting*, vol. 26, no. 4, pp. 700–711, 2010.

[272] D. Fylstra, L. Lasdon, J. Watson, and A. Waren, “Design and use of the microsoft excel solver,” *Interfaces*, vol. 28, no. 5, pp. 29–55, 1998.

[273] W.-K. Wong, M. Manzur, and B.-K. Chew, “How rewarding is technical analysis? evidence from singapore stock market,” *Applied Financial Economics*, vol. 13, no. 7, pp. 543–551, 2003.

[274] P. J. Brockwell and R. A. Davis, *Introduction to time series and forecasting*. Taylor & Francis, 2002, vol. 1.

[275] M. Little, P. McSharry, I. Moroz, and S. Roberts, “Nonlinear, biophysically-informed speech pathology detection,” in *International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, vol. 2. Toulouse, France: IEEE, 2006, pp. II–II.

[276] J. Kornblum, “Identifying almost identical files using context triggered piecewise hashing,” *Digital Investigation*, vol. 3, pp. 91–97, 2006.

[277] Y.-P. Huang, T.-W. Chang, and F.-E. Sandnes, “An Efficient Fuzzy Hashing Model for Image Retrieval,” in *Annual meeting of the North American Fuzzy Information Processing Society (NAFIPS)*, Montreal, Quebec, Canada, 2006, pp. 223–228.

[278] H. W. Lilliefors, “On the Kolmogorov-Smirnov test for normality with mean and variance unknown,” *Journal of the American Statistical Association*, vol. 62, no. 318, pp. 399–402, 1967.

[279] N. Park and W. H. Park, “Cyber threat prediction model using security monitoring system event,” in *IT Convergence and Security 2012*. South Korea: Springer, 2013, pp. 233–239.

[280] S. Qibo, W. Shangguang, Y. Danfeng, and Y. Fangchun, “ARM-CPD: Detecting SYN flooding attack by traffic prediction,” in *2nd IEEE International Conference on Broadband Network Multimedia Technology (IC-BNMT)*, Beijing, China, Oct 2009, pp. 443–447.

[281] H. Park, S.-O. D. Jung, H. Lee, and H. P. In, “Cyber weather forecasting: Forecasting unknown internet worms using randomness analysis,” in *Information Security and Privacy Research*. Springer, 2012, pp. 376–387.

[282] US-CERT. DNS Amplification Attacks - Alert (TA13-088A). Last accessed in October 2015. [Online]. Available: http://tinyurl.com/bp4xud4

[283] M. Anagnostopoulos, G. Kambourakis, P. Kopanos, G. Louloudakis, and S. Gritzalis, “Dns amplification attack revisited,” *Computers & Security*, vol. 39, Part B, no. 0, pp. 475 – 485, 2013.

[284] Dagon *et al.*, “Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority,” in *NDSS*, 2008.

[285] S. Staniford, J. A. Hoagland, and J. M. McAlerney, “Practical automated detection of stealthy portscans,” *Journal of Computer Security*, vol. 10, no. 1, pp. 105–136, 2002.

[286] The University of Waikato. WEKA Select Attributes: Ranker. http://tinyurl.com/kt6rccu [Online; accessed 15-Nov-2013].

[287] T. K. Moon, "The expectation-maximization algorithm," *Signal processing magazine, IEEE*, vol. 13, no. 6, pp. 47–60, 1996.

[288] J. A. Hartigan and M. A. Wong, "Algorithm as 136: A k-means clustering algorithm," *Journal of the Royal Statistical Society. Series C (Applied Statistics)*, vol. 28, no. 1, pp. 100–108, 1979.

[289] D. Hudson, "Interval estimation from the likelihood function," *Journal of the Royal Statistical Society. Series B (Methodological)*, pp. 256–262, 1971.

[290] G. Münz, S. Li, and G. Carle, "Traffic anomaly detection using k-means clustering," in *GI/ITG Workshop MMBnet*, 2007.

[291] J. Yu, Z. Li, H. Chen, and X. Chen, "A detection and offense mechanism to defend against application layer ddos attacks," in *Third International Conference on Networking and Services (ICNS)*. IEEE, 2007, p. 54.

[292] S. Zhong, T. M. Khoshgoftaar, and N. Seliya, "Clustering-based network intrusion detection," *International Journal of reliability, Quality and safety Engineering*, vol. 14, no. 02, pp. 169–187, 2007.

[293] A. Nucci, "Architecture, systems and methods to detect efficiently DoS and DDoS attacks for large scale Internet," Sep. 1 2009, US Patent 7,584,507.

[294] Spamhaus. An arrest in response to March DDoS attacks on Spamhaus. http://www.spamhaus.org/news/article/698/. Last accessed in October 2015.

[295] The New York Times. Firm Is Accused of Sending Spam, and Fight Jams Internet. http://tinyurl.com/bnkmr4c. Last accessed in October 2015.

[296] P. Smyth, "Model selection for probabilistic clustering using cross-validated likelihood," *Statistics and Computing*, vol. 10, no. 1, pp. 63–72, 2000.

[297] Gephi. An open source graph visualization and manipulation software. https://gephi.org/ [Online; accessed 14-April-2014].

[298] Bloomberg News. Dutch Man Arrested in Spain in Probe of Spamhaus Attack. Last accessed in October 2015. [Online]. Available: http://tinyurl.com/lzqheb5

[299] All News Plus. Spam dispute results in biggest ever cyber attack. Last accessed in October 2015. [Online]. Available: http://tinyurl.com/n2ur5ro

[300] Luc Rossini. Twitter: Spamhaus is currently under a ddos attack. Last accessed in October 2015. [Online]. Available: http://tinyurl.com/m7dayxr

[301] Open Resolver Project. http://openresolverproject.org/ [Online; accessed 15-Nov-2013].

[302] CAIDA. Cooperative Association for Internet Data Analysis. Last accessed in October 2015. [Online]. Available: http://www.caida.org

[303] Z. H. Aghaei Foroushani, "TDFA: Traceback-based defense against DDoS flooding attacks," in *28th International Conference on Advanced Information Networking and Applications. AINA.* IEEE, 2014, pp. 710–715.

[304] E. Gansner, B. Krishnamurthy, W. Willinger, F. Bustamante, and M. Snchez, "Demo abstract: towards extracting semantics by visualizing large traceroute datasets," *Computing*, vol. 96, no. 1, pp. 81–83, 2014.

[305] S. Papadopoulos, G. Theodoridis, and D. Tzovaras, "Bgpfuse: Using visual feature fusion for the detection and attribution of bgp anomalies," in *Proceedings of the Tenth Workshop on Visualization for Cyber Security*, ser. VizSec '13. New York, NY, USA: ACM, 2013, pp. 57–64.

[306] A. Wang, A. Mohaisen, W. Chang, and S. Chen, “Delving into internet ddos attacks by botnets: Characterization and analysis,” in *IEEE International Conference on Dependable Systems and Networks (DSN)*, 2015.

[307] M. Bagnulo, P. Matthews, and I. van Beijnum, “Stateful NAT64: Network address and protocol translation from IPv6 clients to IPv4 servers,” *IETF, April*, pp. 2070–1721, 2011.

[308] R. M. Felder and L. K. Silverman, “Learning and teaching styles in engineering education,” *Engineering education*, vol. 78, no. 7, pp. 674–681, 1988.

[309] LOIC. http://sourceforge.net/projects/loic/. Last accessed in October 2015.

[310] Jenny Faig, “Cybercrime: The Risks of Technology,” http://tinyurl.com/pjflg5k, last accessed in March 2015.