Breaking the DDoS Attack Chain

Bryan Harris **Eli Konikoff** **Phillip Petersen**

August 2013
CMU-ISR-MITS-2

Institute for Software Research
Carnegie Mellon University
Pittsburgh, PA 15213

Abstract

Department of Defense (DoD) communications and data networks continue to be targets for adversaries to deny operational use of those networks. Distributed Denial of Service (DDoS) is one such attack strategy that has proven to be an effective method of denying service to military, political, infrastructure, and economic targets. The introduction of botnets as zombies, or computers under control of another entity unbeknownst to the owner, which can be controlled with minimal effort by an obfuscated attacker to degrade or deny usage of networks through overloading capacity, has proven successful time and again. As some network security firms have reported, the United States is a prime target for adversaries, and it is far from impervious to cyber attacks. In their 2011 paper, Hutchins, Cloppert, and Amin discuss the concept of an attacker kill chain for phases of intrusions into networks but do not address other asymmetric cyber threats such as DDoS. In order to fill this gap, this paper provides a survey of the DDoS landscape and examines the application of "kill chain" concepts to the DDoS threat. Leveraging the concepts of detect, deny, disrupt, degrade, deceive, and destroy, the paper explores ways that this chain may be disrupted. Lastly, an overview of the critical and emerging DDoS threats is provided, and considerations are offered for additional technology and research that have potential to significantly reduce the current DDoS threat.

Keywords*: DoD, DDoS, botnet, kill chain*

1 Introduction

Although DoD networks maintain a high sense of readiness and continually monitor and respond to malicious activity, this does not mean they are invulnerable to attacks. A cleverly built botnet that makes its way into the inner circle of these networks is capable of bringing down critical sites that provide command and control to ships, bases, or other command elements If this occurs the ability to maintain an adequate intelligence picture may be impacted, a defense system may be unable to provide the service required to defend the coast of the nation, or some other form of degradation may occur that could ultimately become catastrophic. Abroad, forces may not be able to communicate to ensure mission success. Although command and control for DoD missions is typically performed on classified systems, the use of unclassified systems is often essential for daily operational requirements. Additionally, the nation's critical infrastructure is relied on to provide services such as power, water, and communications transport, and if brought down, could severely impact DoD operations.

Distributed Denial of Service (DDoS) attacks are a popular way to impact people, organizations, and even nations in malicious ways. DDoS is a non-kinetic weapon that is capable of having an effect that is as devastating, if not more devastating, than a well-placed missile. DDoS attacks have been used as a form of retribution, as a means for activists to further their causes, and even as a strategy for a military to create an advantage during warfare. DDoS attacks are defined and described as "many machines" performing a "coordinated" attack where "access to a computer or network resource is intentionally blocked or degraded." [1]. From the hacktivist group Anonymous' DDoS strategies to Russia's purported attacks on Estonia, DDoS is used to thwart the functionality of the servers that are the focus of the attacks [2].

Through a better understanding of the processes used to perform DDoS attacks, defensive measures can be developed to help predict and preempt the successful execution of these kinds of threats. The goal of this paper is to further that understanding by examining DDoS attack strategy so that DoD constituencies can make more informed decisions to defend against these kinds of attacks. Section 2 provides relevant key concepts and offers context for understanding the efficacy of DDoS attacks. In Section 3, a brief history of DDoS attacks and their implications for future decision making is provided. A detailed analysis of the various categories of attackers and the resources these attackers employ to carry out a kill chain or "attack chain" strategy is provided in Section 4. Section 5 explains the "kill chain" [3] model and the strategy used by these cyber attackers, and discusses the concept of "adversary opportunity". A description of the phases as they relate to each stage and various defensive strategies that can break the kill chain through removal of the adversary's opportunities are covered in Sections 6 and 7. In Section 8, an examination of the nation's effectiveness in defending against current DDoS threats is conducted. Section 9 discusses the relative strengths and weaknesses of the current cyber landscape, and examines the potential for emerging threats. Lastly, the direction of future defensive strategies is considered in Section 10.

2 Key Concepts and Context

Distributed Denial of Service attacks come in many shapes and sizes. Typically they are classified according to what they do. Whether it is a volume-based attack that

saturates the available threads for communication, or a protocol or application-based attack that takes advantage of vulnerabilities inherent in the protocol or application, the intent is ultimately to inhibit the availability of the servers or services provided by those servers that are the target of the attack.

One of the reasons these attacks are successful is due to the design of today's Internet. The Internet is designed for speed in delivery of packets and is less focused on security. The responsibility for ensuring security of information on the Internet is pushed to the sender and receiver. Further, according to some sources, the Internet is not designed to police traffic, and thus vulnerable to IP Spoofing [3]. These design features provide multiple opportunities for various kinds of DDoS attacks.

Botnets are often used as the vector of choice to perform DDoS attacks due to the anonymity it provides the attacker as well as the ability to achieve high volumes of traffic with minimal commands being sent. As defined by [4], a botnet is, "a collection of software robots, or bots, which run autonomously and automatically. They run on groups of zombie computers controlled remotely by attackers." These "bots" are a source of "capability" that aids an attacker in his or her endeavor to perform malicious activity. The relationship to the kill chain strategy is discussed further in Section 5.

3 History of the DDoS Attack

DDoS attacks existed prior to 1998 but the first recorded automated DDoS attack toolwas discovered by CERT in 1998 and named "fapi" [5]. This was a very primitive tool compared to today's tools, but at the time so were the networks of the world. By 1999 the tool set had morphed into a more sophisticated and controllable set of tools called "Trinoo" and "Tribe Flood Network." These tools allowed communication between a centralized node and the compromised nodes through encrypted channels that added to the anonymity of the attacker. The first confirmed DDoS attack was on an ISP known as Panix in September 1996 [2]. By comparison to modern day attacks this is very primitive and would be easily traceable with today's forensics tool kits. However, as the ability of the defender increased and the tools to perform forensics became more advanced, the attacker's level of sophistication also increased.

In 2007 and 2008 multiple Russian actors were accused of using cyber attacks against Estonia and Georgia respectively [2]. The attack on Estonia was politically motivated by a disagreement of the relocation of a Soviet statue. In the case of the attack on Georgia, this was a political attack that had an element of propaganda in favor of Russia [6]. Both of these attacks had significant impact on the command and control of the attacked nations. These attacks both involved large botnets with Russian based command and control nodes, which were more focused in intent than some of their predecessors.

According to a McAfee report, [7] an elaborate DDoS attack occurred in March of 2011. The attack used various forms of encryption and a multi-tiered distributed botnet within South Korea to attack approximately 40 different websites belonging to the South Korean government and U.S. military forces in Korea. According to McAfee the intent of the attack was "to slow analysis and ultimately increase time to mitigation." Alternately, McAfee theorizes that this was possibly an effort by the attacker to measure these same capabilities of the South Koreans and U.S. forces, and ultimately assess their "preparedness" for cyber attacks.

Operation Abibil was a set of DDoS attacks that occurred from December 2012 to early January 2013. These attacks were perpetrated by a hacktivist group known as Izz ad-Din al-Qassam Cyber Fighters (QCF) in response to the YouTube video "Innocence of Muslims" [8]. The targets of these attacks were multiple entities in the financial industry and resulted in inaccessibility to the associated web sites. The QCF wanted the video removed and chose the DDoS attack as the means for achieving their hacktivist objectives. It is important to note that hacktivists can use social media as a means for recruitment to build a large attack force rather than seek out the services of botnets. Anonymous has performed recruitment over Twitter and Facebook for multiple attacks throughout time. This sympathetic group is equally if not more capable of performing a DDoS attack depending on the magnitude of recruited people.

One of the more recent DDoS attacks was in March 2013. Spamhaus, an anti spam company, was attacked with a large DDoS attack that was on the magnitude of 10Gbps initially followed by 100 Gbps of traffic. Spamhaus had enlisted the services of CloudFlare to try to stop the DDoS attack. CloudFlare reported that the attackers changed tactics when their attempts failed to bring down Spamhaus. The attackers focused on upstream providers of Cloud Flare that resulted in a rate of 300 Gbps traffic and nearly took down the Internet Exchange points [9], which could have brought down the Internet as a whole.

The attack strategies described above provide a snapshot of some of the DDoS attacks in recent history, but they are not all-inclusive. There are many attacks that go unreported or are failures and receive no mention in collected metrics. The historic examples exemplify the changing dynamic of the DDoS attack over time. It is not only the tactics that have evolved it is the reason for use of the attack that has changed as well. Whether it is the military advantage that can be gained or the advancing of an activist cause, the DDoS attack has allowed attackers the capability to morph their intent into concrete actions with viable impact.

4 Attack Chain Categories and Resources

According to Arbor Networks, the top three most commonly perceived motivations for DDoS attacks are "political or ideological, online gaming and vandalism/nihilism. These are largely acts done in reaction to real or perceived offenses" [10]. Other researchers have proposed that there are two general categories of attackers: nation state based and non-nation state based. Each has different levels of capability and motivations for their attacks. Nation state based attackers have implicit protection, if not authorization, from the host country. In some cases they leverage training and resources provided by the government but are equally likely to be contractors supporting the government [11]. In addition to making political statements, nation states can also use DDoS attacks coupled with kinetic attacks to maximize the effectiveness of an attack on an adversary's crippled C2 system [12].

Non-nation state based attackers are those groups such as LulzSec or Anonymous who are comprised of likeminded activists and have a mix of skill sets as simple as ordinary Internet users to as complex as highly skilled

hackers. These so called hacktivists are typically focused on making a political or ideological statement such as the attack on FBI for the shutdown of the popular Megaupload website [13].

Terrorist organizations such as Al Qaeda have benefitted from hacktivists such as the "Mauritania Attacker", a member of AnonGhost, whose cyber activities are based upon the notion of fighting for Islam using peaceful means [14]. However groups such as these should not be confused with the type of cell that would be responsible for IEDs or physical attacks on targets. A final non-nation state based attacker is the criminally oriented profiteer whose goals include commercial espionage, extortion and manipulation such as the Russian Business Network (RBN) and the Rock Phish Gang [15].

Additional distinctions can be made within the two general categories of attackers. The most recent Defense Science Board (DSB) report [16] identifies six tiers of attacker described as follows:

- Tiers I and II attackers primarily exploit known vulnerabilities
- Tiers III and IV attackers are better funded and have a level of expertise and sophistication sufficient to discover new vulnerabilities in systems and to exploit them
- Tiers V and VI attackers can invest large amounts of money (billions) and time (years) to actually create vulnerabilities in systems, including systems that are otherwise strongly protected. Tier V and VI attackers are typically associated with nation states such as China, Russia, Israel, the United States and most recently Iran.

5 The Kill Chain (Attack Chain) Strategy

The "intrusion kill chain" or "kill chain" from the Lockheed Martin paper [3] is used to describe a methodology or model by which an adversary engages a specific target to further malicious intent. The use of "attack chain" is referenced in this paper as well and is synonymous with the terms in the Lockheed Martin paper for the purpose of reading. The model follows the Table 1 format below with the associated definitions paraphrased from that paper. The full definitions are included in Appendix A for reference.

Reconnaissance	Research, identification and selection of targets.
Weaponization	Coupling software such as a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer).
Delivery	Transmission of the weapon to the targeted environment.
Exploitation	Root access to a host machine through a security vulnerability, which allows execution of malicious code.
Installation	Addition of files and executable code such as a remote access trojan required for the adversary to maintain control over the host machine.
Command and Control (C2)	The process of directing the activities and actions of a host machine by the botmaster.
Actions on Objectives	Activities originated by the botmaster in the C2 stage, which are directed against a target or other hosts.

Table 1. Steps of the Kill Chain

This paper focuses on each of these steps in detail in order to discuss how a defender can remove or minimize the "opportunity" of an adversary and thus remove the threat as discussed in the threat triangle discussion below. It suffices to say that when this opportunity is removed the threat will cease to exist. Ultimately, this means continuity of operation of networks, even under hostile or targeted conditions.

Similar to the "fire triangle" that highlights the 3 necessary components to create fire (heat, oxygen and fuel) an analogy can be made for a "threat triangle' that includes the three required elements to generate a cyber attack: intent, opportunity, and capability [17] (Figure 1). As with the "fire triangle," if any of the legs are removed from the "threat triangle", the overall threat is neutralized. To apply this framework to cyber security, if an adversary's capability, intent, or opportunity is neutralized or removed, the adversary is incapable of causing large-scale harm to operations.

Figure 1

Examples of how to neutralize an attacker's capability and intent are, respectively, kinetic strikes on infrastructure, and psychological operations on personnel. There are multiple other options but they are equally as difficult, potentially perceived as hostile, and are outside the scope of this paper. This paper focuses exclusively on the possibility of reducing the "opportunity" leg to near zero availability. However, there is no simple solution to achieving this goal due to the dynamic nature of the vectors of attack and the growing demand for seamless connectivity.

For our purposes, the attack chain model from the Lockheed Martin paper discussed above is comprised of an iterative cycle similar to that described in the Mandiant report [18]. As can be seen in figure 2, the cycle starts with reconnaissance followed by the remaining steps described above in Table 1. It is important to understand that action is not necessarily required in each phase of each stage of this cycle. Section 6 and 7 will leverage this iterative

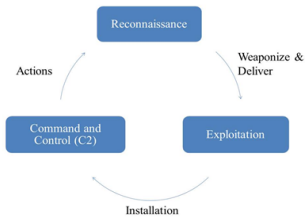

Figure 2. Attack iteration

cycle to show a two-stage approach to how a DDoS attack can be performed. Stage I focuses on building or renting a botnet to create the "capability" leg of the Threat Triangle. Stage II builds from Stage I, and demonstrates how an adversary will again use the cycle above to perform the remainder of the attack. Included in the discussions are defensive mechanisms or proactive measures that may be leveraged in order to "Break the DDoS Attack Chain" and preserve normal operations of networks.

6 Stage I: Build a Botnet

By definition the distributed aspect of the DDoS attack requires access and control over a large number of hosts or bots. Today, access to botnets for uses both good and bad is readily available. The technical barrier to building a personal botnet is extraordinarily low thanks to toolkits such as Dirt Jumper and its follow on, Pandora, which can be found online for as little as $800 [19]. If money is an issue a cracked version is likely available somewhere in the underground market for free or at a significantly reduced cost. Utilizing a rented botnet, tools such as Pandora can be a one-stop shop for building your own botnet without requiring the traditional, more manual legwork.

For the true do it yourself type there are "how to" articles describing all of the individual tools required and how they need to work together to build a bot-net from scratch for less than $600 in start up costs and less than $200 per month to maintain. These costs include a VPN and hosting server for C2, domain names with fast flux service, botnet and exploit toolkits and delivery services to the victim machines [20]. Those not inclined to go through all that effort can simply rent a botnet for as little as $10 for one hour of DDoS service on the target of your choice [21]. Reference [22] provides a comprehensive taxonomy for the lifecycle of botnets distinguished by the phases of development (e.g., injection and spreading, C2 and application). The injection and spreading phase correlates well to the first five stages of our attack chain. A further breakdown of the phases includes propagation, communication and attack methods and ways to make the bots more resilient to discovery and destruction. For reference, figure 3 from [22] on the following page shows the basic life cycle and taxonomy of a botnet.

Botnet life cycle			
Phases		Instances	Resilience techniques
Injection & Spreading		-Distribution of malicious emails -Software vulnerabilities -Instant Messaging -P2P File sharing Network -Other Botnets	-Using trusted process -Trivial name-based obfuscation -Rootkit Techniques -Reduce Security rules -Reduce system capability -Installing antivirus software -Incorporated antidebugging & antivirtualization -Variant Spreading Techniques -Polymorphism & Metamorphism -Continuous bot upgrade
Command & Control	Model & Topology	-Centralized »Single Star »Multiserver Star »Hierarchical -Distributed »Random	-DNS techniques -Multiple URLs -Encryption Techniques -Dead drop -Variant C&C
	Application & Protocol	-IRC -HTTP -IM -P2P	
	Communication initiation	-Push Method -Pull Method	
	Communication direction	-Inbound -Bidirectional	
Botnet application		-DDoS attacks -Spamming & Spreading malwares -Espionage -Hosting malicious applications & activities	-Exposure limitation -Retaliation techniques -Camouflaged messages - Anonymization techniques

Figure 3. Taxonomy

This taxonomy provides a useful tool for communication between the various stakeholders involved in defense of DDoS attacks. As stated in the description of the Threat Triangle in Section 5, the capability leg for using botnets is difficult to remove. Considering the relative inexpensive nature of building a botnet or renting one for use and the significant role it plays in the DDoS attack chain having a common language to discuss the problem is of great value.

6.1 Reconnaissance

The first phase in building a botnet requires reconnaissance of the targets. It is important to note that the target for bot recruitment can be personal computers as well as data centers full of servers with significantly more processing power and bandwidth at their disposal. In either case, development of a botnet involves searching for hosts with vulnerabilities, which can be exploited for installation of malware, usually Trojans, with backdoors for further manipulation and command and control of the machine. Advanced Google searches or "Google Hacking" described by Johnny Long in his book "Google Hacking for Penetration Testers" are possible manual methods to conduct this search.

Digital signatures of known malware can be used to block malware intended to create bots via firewalls or other inspection platforms. Other approaches of some value are the implementation of local network policies blocking certain types of traffic such as Internet Control Message Protocol (ICMP), blocking traffic from Tor nodes and host based security agents which are capable of assisting in thwarting the intentions of a botnet creator through policies and known host behaviors and activities. Education of users on the tactics and techniques botmasters use to create their weapons can be of significant value since it potentially prevents the addition of another bot to the army and another source for further recruitment. Honeypots comprised of decoy machines and systems can also be useful to gather information and determine the attack methods being used for future analysis as well as establish and countermeasures with the potential benefit of being able to trace back [23] and destroy the botnet.

6.2 Weaponization

The vast amount of open source toolkits and relative free information on the Internet prevents a significant impact of defenses against the weaponization of software [24]. An intelligence approach of gathering information and monitoring forums for requests for help or information regarding the creation or access to botnets may assist in preventing middle to lower tier attackers. However, little if anything can be done to stop a skilled attacker from writing his or her malicious code on a personally owned computer for later delivery and exploitation. From the perspective of a software manufacturer, improved security practices and standard configurations (e.g. service off by default) would assist in reducing the number of possible exploits available for attackers to target.

6.3 Delivery

Once malicious code is weaponized or purchased the software can either be delivered via a spam campaign containing the software or through the victim's selection of links within the spam or phishing message to seemingly genuine websites containing the malicious code for download and execution. Another possible avenue for delivery is the use of a worm similar to the Storm worm [25]. The DoD is not immune to these attacks as was demonstrated by the Welchia worm in 2003 [26]. Because these worms typically exploit a particular vulnerability in an operating system or other piece of software, the homogeneity of systems (e.g. common hardware and software environments) may increase the ease that such a worm is able to propagate across multiple systems. This homogeneity is a concern that some security experts have expressed as organizations seek to find cost-savings through the standardization of their information systems [27].

With regard to defending against the delivery of such malware, digital signatures can be used to identify and prevent the installation of known malware. However, the use of polymorphic and metamorphic transformation engines can render this technique useless. Malware changing its code through encryption and appending or prepending data is considered polymorphism. Metamorphism is the act of malware automatically changing itself each time it propagates to another machine [22]. To combat this shift in attack new techniques isolating and identifying the engines used to morph the malware are being used [28]. Here again, user education to prevent inadvertent selection of the link or opening of the file is of value. One study indicated awareness-creating activities are more effective than the technical measures implemented by organizations for information security [29].

6.4 Exploitation

The exploitation of would be bots is made possible through unpatched software vulnerabilities, insecure software coding practices, disgruntled employees and a lack of user education or attention to detail. If kept up to date, the use of anti-virus software is effective against malicious code with known signatures and established vulnerabilities. Again, the use of polymorphic transformation engines drives the need for more advanced characterizations of malware in order to prevent their spread. Security software installed locally on the host such as Host Based Security Systems (HBSS) which is currently implemented by the Defense Information Systems Agency (DISA) can assist in detecting and therefore preventing installation of the package [30]. Additionally, application white listing can be leveraged to allow the user to explicitly control the executables that are run on the host by comparing applications attempting to run on the host machine with the known application database. In this way, even zero day exploits can be prevented [31]. Mitigation strategies such as forced diversification of the network to avoid the pitfalls of computer monoculture may also be effective. Finally, for those computers that can be physically manipulated a manual setting of the jumpers on the BIOS to write only can prevent more permanent damage to the victim machine [32].

6.5 Installation

Similar to the defenses for the exploitation phase, Host-based Intrusions Detection Systems (HIDS), HBSS and application white listing all provide some level of defense against this phase of the attack. Implementation of a change root jail can effectively prevent an attacker's malware from having access to the portion of the file system required to complete the installation.

6.6 Command and Control (C2)

After the weapon has been successfully installed and beacons to the botmaster, the target is officially controlled by the botmaster. Usually, the initial delivery and installation of malware is only enough to allow the bot to communicate with the C2 node so that it can download the full package of malware. In this way bots can be sure to download the latest versions of malware desired by the botmaster. From this point forward the machine will do the bidding of the botmaster whenever it is online until the infection has been detected and mitigated by the administrator. Typically, compromised hosts must beacon outbound to an Internet controller or server to establish a C2 channel [3].

Botnets can be divided into two basic types characterized by their C2 architecture; centralized and decentralized. Centralized botnet C2 architectures were the most popular format early on using Internet Relay Chat (IRC) for a relatively simply design. Shortcomings of this approach include a single point of failure and greater ease of detection. Decentralized architectures include Peer-to-Peer (P2P) styles, which trade off additional complexity for a more robust and survivable botnet for the botmaster to control. Numerous surveys containing more detailed descriptions of both the technologies used and defenses exist. One such survey [32] includes an additional, theoretical characterization titled "unstructured" in which each bot would only know about one other bot. Though highly resilient to sabotage, a significant amount of latency would necessarily exist within this architecture.

Two broad categories of defense can be used for botnet detection; host based and network based. Each approach has its own set of advantages and drawbacks however, just like in the case of an overall defense strategy, the importance of a layered approach of complementary defenses cannot be understated. Host based security systems can monitor and track local behaviors and have access to data in its unencrypted form but is unable to correlate that information across the network to determine its role in network behaviors. Network based security systems have the advantage of seeing all the traffic flows across the Local Area Network (LAN) or Wide Area Network (WAN) and can utilize that information to detect larger patterns within the network. Since the data flows will likely be encrypted the network based system will not have access to that lower level

detail. The combination of these two approaches provides the optimum solution for detection. Botminer and Botswat are a few of the implementations used to detect the existence of botnets on the network and host respectively. Botminer is a protocol independent tool, which detects bots through network traces to identify malicious activity patterns [33]. Botswat is a host based behavioral detection tool, which applies library call level taint propagation to distinguish between locally initiated and remotely initiated activities [34]. A more extensive treatment of botnet detection techniques can be found in [35] and [36].

Two more methods of botnet discovery and dismantling are usage of packet traceback and leveraging of the legal system. Packet traceback techniques, such as those proposed by Snoeren et.al [23], utilize a hash based packet marking strategy to create an audit trail capable of identifying the origin of a single packet even when IP spoofing is used. As for using the legal system, as recently as June 5, 2013 the FBI, with assistance from Microsoft, identified and seized two servers in New Jersey and Pennsylvania to disrupt more than 1,000 botnets responsible for an estimated $500 million in consumer and business losses [37]. Previously, Microsoft was part of a team who was successful in completely dismantling the Rustock botnet responsible for spam attacks through a similar approach [38].

6.7 Actions on Objectives

Once the C2 channel has been established attackers have complete access inside the target environment. At this point the creator of the botnet can do what he or she would like. The botnet could be rented out for use by others or kept for the creator's own personal use. Commands can be sent to upload additional software to send spam, capture keystrokes and sensitive information for later use or execute DDoS attacks on a future target. Defenses against these actions are a culmination of all the previously discussed techniques. Host and network monitoring tools, honeypots and legal actions are all possible mechanisms to prevent, detect and defend against the activities of the botnet. Last, the application of offensive cyber operations to counter attack or preempt an identified assailant is considered a viable option by nation states [39].

7 Stage II: Commence DDoS attack

Stage II of a DDoS attack consists of the phases that an attacker takes to perform a DDoS attack once they have access to a botnet. As mentioned in section 5, Stage II of the DDoS attack chain differs in several ways from Stage I and may even skip several steps of the attack chain model described by Lockheed Martin [3]. In Stage II of a DDoS attack, the attacker has significant freedom of movement prior to the delivery of the attack and there may be little intelligence indicating an attack is to occur since most preparation occurs with little to no interaction with the target(s). An attacker can lie in waiting, conducting reconnaissance anonymously while developing a DDoS strategy to use against their target. To conduct their attack, they will use a botnet that they constructed or rented as in Stage I, and, with little warning, strike a target by sending commands to their botnet.

Mirkovic and Reiher [40] break DDoS defense measures into two broad categories: preventative and reactive. Preventative measures can be further categorized into the categories of attack prevention and DoS prevention measures. Attack prevention measures are those that deal with designing and modify systems and Internet protocols to eliminate the threat of DDoS altogether. This includes general system security and ensuring that industry best practices are followed, (e.g. vulnerability patching, firewalls, and intrusion detection and preventions systems) as well as protocol security (e.g. ensuring that protocols are designed in a way that they are more difficult to take advantage of to perform a DDoS attack).

DoS (Denial of Service) prevention measures on the other hand, focus more on the resiliency of a system, and allowing the victim to endure an attack without loss of service through. DoS prevention measures include resource management, adding additional resources, or physical distribution of resources. Reactive measures aim to lessen the impact of an attack. Attack response includes identifying the attacking agents, rate limiting, filtering, and network topology reconfiguration. As history has shown, no single method is likely to be completely effective or able to completely eliminate the threat of DDoS attack, so a layered defense approach is ideal. Reactive mechanisms focus on the detection and response to a DDoS attack. Detection is generally performed through pattern or anomaly detection [40].

7.1 Reconnaissance

The first phase that an attacker must make when attacking a target is to find specific vulnerabilities or services they wish to bring down. Potential targets could be web servers, application servers, individual hosts, resources, networks, or even large-scale infrastructure targets. For an attack to be most effective the attacker must gain an understanding of their target's network configuration to find particular vulnerabilities, critical services, network chokepoints, or other network vulnerabilities. This reconnaissance is performed using various methods, including the use of Open Source Intelligence (OSINT) or tools available for free on the Internet to scan and analyze target networks. Nmap is one popular reconnaissance tool that provides scanning and network discovery features capable of determining network details such as hosts available, services, Operating Systems (OS), firewalls, and more [41] [42].

Maltego is another tool that is able to search through a variety of widely available information on the Internet in order to fingerprint a network, which could allow an attacker to find critical points in a network [41]. There are also a number of other vulnerability scanning tools available for free or sold by security companies include tools such as Netcat, SuperScan, Nessus and others [41]. While these tools are powerful, if the attacker is not careful, and if the target has implemented sufficient defenses, then these scans could be detected or prevented through the use of Intrusion Detection and Prevention Systems (IDPS). Anonymizers such as Tor are tools that may be used by an attacker to prevent targets from determining where scans are originating from and make it nearly impossible to trace back any packet traffic to the source [41].

There are a number of measures that can be performed to prevent network reconnaissance from occurring on the target network. Network Intrusion Detection Systems (NIDS), IDPS and firewalls can be implemented to help block this reconnaissance traffic or to detect scans as they occur. One popular open source NIDS is Snort, which is able to detect many of these scans [41]. As in Stage I, blocking Tor exit nodes may also be an option (if operations permit) to help

prevent anonymous reconnaissance on the network. Lastly, following industry best practices on network configuration can greatly reduce the ability for attacker to find and collect open source information or other information about the target network.

7.2 Weaponization

The weaponization phase of Stage II consists of the attacker actually designing an attack. The attacker could take advantage of existing tools and vulnerabilities or they could design a new, never before seen, zero day attack. Types of attacks can be broken down into two broad strategies: protocol attacks and volumetric attacks, though many can be considered hybrids, having characteristics of both protocol and volumetric attacks [40]. Defenses against the weaponization include attack prevention mechanisms that make attacks obsolete or ineffective against a target system, thus reducing the number of effective options that an attacker has when attacking a target [40].

Protocol attacks, also known as semantic attacks, target a specific feature, implementation or protocol flaw or vulnerability in a network, server, or application [40]. By taking advantage of these flaws, an attacker may be able to successfully deny service to the victim using far fewer resources than may be required for volumetric attacks. Example attacks include fragmentation overlap attacks such as the Teardrop attack that was first seen in the late 1990's, or more recently, the Low-rate DoS attack (LDoS) that exploits the TCP retransmission timeout mechanism in routers in order to disrupt traffic flow [43] [44]. Attacks utilizing Internet Control Message Protocol (ICMP) take advantage of the control channels of the Internet using ICMP error messages to cause connection resets, throughput reduction, and performance degradation. Descriptions of ICMP attack types—as well as their countermeasures—are outlined in IETF RFC 5927 and are largely preventable if networks are properly configured [45]. Application layer attacks are increasingly popular type of protocol attack that targets specific attributes of web applications in order to exhaust server resources. The advantage of these attacks is that they often take relatively few resources compared to traditional denial of service attacks, and can potentially be carried out by a single host [46]. Application layer attacks are described in further detail in section 8.3.

In a volumetric attack, also known as a brute force attack, a large quantity of traffic is directed towards a target server in order to flood and overwhelm the victim's network, server, or application resources. Rather than taking advantage of a flaw in a protocol, these attacks attempt to consume the victim's resources with spoofed traffic so that they are unable to process legitimate traffic [47]. Examples of volumetric attacks include UDP, ICMP, and IGMP floods, all of which involve sending large numbers of packets to target servers in order to consume bandwidth and sever resources. Attackers may attempt to reflect and amplify attacks using spoofed packets, as in the case of the Smurf Attack, or more recently, through the use of DNS amplification attacks.

DDoS defense service providers such as Cloudflare have seen an increase in these DNS amplification attacks, as it allows attackers to utilize the large public DNS servers to reflect and amplify traffic to a target [46]. DNS amplification attacks are performed by sending relatively small DNS zone request packets to public DNS servers where the return IP address is spoofed with the victim's IP [46]. The DNS server then replies to the spoofed IP address (the victim's server) with a reply packet that is up to fifty times larger than the request packet [46]. An example of such an attack is the attack against Spamhaus described in section 3 of this paper.

Hybrid attacks have characteristics of both protocol and volumetric attacks, and typically target weak points in protocols by overwhelming them with traffic or requests. These attacks may require more data to be sent than in a standard protocol attack, but may be able to deny service to a target with far less attack bandwidth than may be required in a strict volumetric attack [40]. Examples of these attacks include SYN flood attacks, which take advantage of the three-way handshake of Transmission Control Protocol (TCP) by only completing part of the handshake and thus leaving half-connections open on the target device. If enough of these half-open connections are made, resources at the target server may be overwhelmed and unable to establish connections with legitimate users [40]. A similar attack that targets the application layer is the Slowloris attack taking advantage of webservers by keeping connections open using partial Hypertext Transfer Protocol (HTTP) requests, again overwhelming server resources with few resources required on the attacker's side [48].

Attackers have a number of tools at their disposal when architecting a DDoS attack. Botnet Toolkits toolkit such as Dirt Jumper and Pandora come with the capability to perform number of types of DDoS attacks. Dirt Jumper for example comes with the ability to perform a number of types of attacks, including HTTP Floods, Synchronous floods, Downloading Flood, and more [49]. The Pandora toolkit improves on Dirt Jumper, including HTTP Min, HTTP Download, HTTP Combo, Socket Connect, and Max Flood attacks, as well as the ability to specify additional settings for the bot that give the attacker more control over how the attack is carried out. [49]. Custom built toolkits could potentially allow for even more advanced botnet capabilities, such as the N^2 attacks, described in Section 8 of this paper. Other tools, such as Low Orbit Ion Cannon (LOIC) and Slowloris are available freely for anyone to download. These tools can be used to perform application layer flooding attacks and may be able to successfully perform a denial of service from only a single host. When used in an organized manner by multiple users and thus distributing the attack sources, these attacks can become even more powerful [48] [41].

Methods of disrupting the weaponization stage consist primarily of preventative measures. Mirkovic and Reiher define attack prevention measures as those mechanisms, "that modify systems and protocols on the Internet to eliminate the possibility of subversion or of performing a DDoS attack" [40]. By eliminating the possibility of a particular DDoS attack, it effectively reduces the number of tools attackers have in their toolbox. If a particular protocol is no longer vulnerable, or a system is configured in such a way to make a particular attack useless, it forces the attacker to move to other attack methods that may be less effective or develop new methods. Preventative measures act primarily as defenses against semantic attacks through the addition of protocol security mechanisms and through proper network configuration. Brute force attacks are more difficult to prevent outright, and must be mitigated using the defense mechanisms outlined in section 6.7.

7.3 Delivery, Exploitation, and Installation

Due to the nature of DDoS attack, and because the botnet is established during Stage I, the attacker is not looking to deliver malicious software or exploit vulnerable hosts in this stage. If the bots already have the attack software required, then the attacker can move directly to the Command and Control phase of Stage II. However, if the attacker needs new or updated software to perform their attack, they may revisit the Stage I installation phase to install this new software [50].

7.4 Command and Control

The Command and Control (C2) phase in Stage II of a DDoS attack consists of a botmaster communicating with their botnet and giving the bots directions for an attack. These directions utilize the C2 channels established in Stage I and carried out in the manner determined in the weaponization phase. As an attack progresses the attacker may continue to return to this stage to modify their attack as necessary to change targets or attack strategy. Depending on the complexity of the DDoS software installed on the bots, the botmaster may need to communicate with the bots for any change in the attack, or as is possible more advanced bots such as Dirt Jumper and Pandora, a complex string of commands may be given to each bot determining when, and how and who to attack at various intervals, allowing a complex attack to be choreographed with little to no interaction required by the botmaster [49].

In general, the methods of disrupting botnet C2 given in Stage I also apply to disrupting Stage II C2. The primary distinction that will be made here is that disruption in Stage II means disrupting botnet C2 of an ongoing attack. Once the attack is underway, there is the potential for an increase in C2 traffic, though this may or may not be the case. Just as in Stage I, if the attack source can be identified, it may be possible to disconnect them from the network through cooperation with ISPs or other methods.

7.5 Actions on Objectives

During this stage, the attack is ongoing. Bots are performing the attack as designed by the attacker using the methods and tools described in section 6.2. There are a number of methods of defending from and mitigating an ongoing attack. Mitigation techniques, such as globally distributed servers and load balancing allows the defender to shift resources around to various servers, forcing an attacker to spread their attack resources amongst multiple targets. Defenses against DDoS attacks can be characterized as occurring in one of three places: on the victim's end, on the attacker's end, or somewhere in the networks in between. Defense at each stage has it's own advantage, but a multi-tiered, defense-in-depth approach is likely going to provide the most complete defense. For the purposes of this paper defenses during this stage are characterized by the location that they take place.

Victim-end defense includes mechanisms that are employed locally on a network to defend from DDoS attack. Some of the more popular of these mechanisms include intrusion prevention systems (IPS) and packet filtering. These mechanisms aim to identify malicious traffic and to block it from the network either manually identifying malicious traffic through signatures, or through traffic analytics. Products such as Arbor Peakflow SP Threat Management System (Peakflow SP TMS) aim to identify and remove DDoS attack traffic while letting in legitimate traffic. However, these systems also have numerous disadvantages, including potentially filtering legitimate traffic. These defenses alone may also act as a bottleneck in a volumetric attack. [51]. Another strategy some organizations may use is simply increasing available network and server resources that allows them to handle more traffic, thus requiring additional resources by the attacker in order to take down a server or network. However, with the size of volumetric attacks continuing to increase significantly, other off-site defense measures may need to be considered in addition to these on-site mechanisms.

Intermediate network defense mechanisms occur somewhere in the networks between the attacker and the victim. These defense mechanisms aim to prevent DDoS traffic from ever reaching the target network. This may be particularly useful in the case of volumetric attacks that exceed the capacity of a local network, and therefore no amount of filtering could prevent local routers from being overwhelmed [46]. One method is the "Clean Pipes" method, where data is "cleaned" at upstream routers that may have greater network capacity and can therefore filter more data than the typical victim could filter [52]. These services are provided by numerous service providers and security companies such as Prolexic [53], AT&T [54], and Verisign [55]. Another approach that can be taken is the use of a detection scheme amongst multiple Internet routers and switches that are able to analyze network traffic and detect when a DDoS attack is occurring. This has the potential to be very effective in countering DDoS attacks, but requires collaboration between service providers and the owners of Internet routing equipment to fully implement. The Cloud Signaling Coalition is a group of security companies and service providers around the world that is attempting to promote this concept in order to provide a more intelligent, collaborative defense method against DDoS attacks [56].

Source-end defense mechanisms aim to stop DDoS attacks at the source of the attack. By controlling the data flow from an attacking computer, the excessive or malicious traffic can be stopped at the source. While this is the ideal defense to a DDoS attack, in reality it is perhaps the most difficult problem to solve. Not only can spoofed IP addresses make it difficult to actually detect bots, but also the sheer number of bots only complicates things further [51]. Collaborative intelligence gathering by service providers as described in section 6.5.2, as well as methods to detect and disrupt command and control to bring down attackers at the source are potential methods to target DDoS attacks at the source. However, this requires significant intercompany and international cooperation to be effective.

8 Evaluation of Current Effectiveness

Traditional defense mechanisms are still reactionary rather than proactive. For the Department of Defense (DoD), entities such as the Defense Information Systems Agency (DISA) and the subordinate commands that provide traffic conduits have at their disposal blacklisting of IP addresses and procurement of more equipment as a means of defending against DDoS attacks. Blacklisting every IP that appears to be part of an attack is cumbersome for the system administrators and often impossible depending on the level of traffic, not to mention the possibility of this blocking legitimate traffic.

Likewise, changing the infrastructure of an organization to increase capacity may prove to be costly or infeasible due to the size of the network. Provisioning of

services of an entity that can provide the level of equipment needed to adequately defend a network is often required by organizations to ensure continuity of their operations in the face of a DDoS attack without having to rebuild their own infrastructure. Businesses such as Akamai or CloudFlare [9], as well as others, provide this service for a fee. Often the fee is related to the level of network traffic the defended organization typically has. This moves the DDoS protection responsibility to a separate entity and allows the organization to continue to operate its business to meet its missions.

The DoD is no stranger to this DDoS threat as they operate servers that are accessible and often may provide critical services to enable mission success. The Lockheed Martin research paper [3] suggests developing an Intelligence driven model to thwart would be attackers but this is of limited use for the DDoS attack. One reason is that the DDoS attack is dynamic in nature and evolves with the technology that emerges throughout time. Another reason is that a DDoS attack is usually the final attack the aggressor will make and not a precursor to a follow-on attack. However, this does not preclude using the intelligence model on the battle space preparatory attacks that are the precursors to the DDoS such as scanning, spamming, and malware introduction.

An evaluation of our nation's effectiveness in combatting DDoS attacks on its networks is necessary to determine where we stand in the cyber security arena. However, as discussed previously, the dynamic nature of the DDoS attack makes it difficult to capture metrics on the effectiveness defensive strategies, or the availability of services as a whole. Due to differing sizes of organizations, network infrastructures, policy implementation, and budgetary concerns, these metrics are better served for reporting to individual organizations rather than being used as a consolidated assessment of the nation's ability to defend against these kinds of cyber attacks. As such, prevention and availability, as a nationwide metric, are typically not reported on in quarterly reports by companies such as Prolexic, Arbor Networks, or Akamai. This does not preclude those companies from reporting on individual companies in their case studies. Also of note is the fact that these companies are reporting on information that is relevant to them and their customers and not on the U.S. as a whole. As there is no single entity that is responsible for Internet security for the United States, the reported numbers are snapshots that are representative of only a sample of the country's cyber defense mechanisms.

Prolexic is a company that is specifically charged with the responsibility of defending against DDoS attacks for its customers. They maintain a cloud infrastructure that is the front end for many global companies as well as government agencies. They are capable of diffusing large scale DDoS attacks across their infrastructure in order to ensure continuity of operations of its customers. Their First Quarter 2013 (Q1) report [57] provides insight into where they are today and compares some of the statistics over the last year. They noted that 2013 was a "landmark year for DDoS attacks." Specifically, Prolexic noticed a change in tactics from application layer based attacks to layer 3 and 4 Infrastructure and capacity attacks. The break down of these attacks for the Q1 report is 23.46 percent and 76.54 percent respectively. With this, Prolexic noticed that the duration of attacks were averaging 34.5 hours, which was an increase from 28.5 the previous years. Prolexic reported that the number of attacks overall had increased 21 percent and that the bandwidth of these attacks had increased by 691 percent from 6.1 Gbps (gigabits per second) to 48.25 Gbps on average. Prolexic points out that this increase in bandwidth is reflective of, "how the power of botnets has increased over the last 12 months." One of the more disturbing issues that Prolexic noticed however was the increase in attacks using higher rates of packet traffic on ISPs (Internet Service Providers). 32.4 Mpps (mega packets per second) was not a staggering number but it was reflective of a change in tactics of the adversary to focus upstream of the people that are charged with the defense of their customers.

Arbor Networks is similar to Prolexic in that they provide network security solutions to customers ranging from large-scale enterprises to global ISPs. Arbor utilized ATLAS® (Active Threat Level Analysis System) to perform a survey of 250 of its customers to gain a perspective on "Internet security and traffic trends" [10]. It was no surprise that DDoS remained the number one perceived threat to these customers. These customers on average had seen a significant increase in DDoS activity whether it was personal or to one of their own customers. 75 percent had seen DDoS attacks to their customers and greater than 50 percent had seen attacks on ISPs similar to the Prolexic discussion above. Arbor Networks noted that slightly under half of its customers had seen actual outages from DDoS attacks. Arbor stated that this, "demonstrates the disparity in defense capability that Internet operators have available." Arbor reports that the peak attack has decreased from 100 Gbps in 2010 to 60 Gbps in 2012 but the average attack sizes have grown in that time period at greater than 1 Gbps. Arbor attributes these numbers to a changing dynamic in the way adversaries are attacking using DDoS. Unfortunately, Arbor noted that there has been an increase in customer utilization of firewalls as a means to defend against DDoS attacks. Firewalls are known to be inefficient at actually performing this defense based on the way they maintain session states.

Akamai is a company that provides network services, which includes the defense of customer networks from DDoS attacks. Akamai's 2012 report [8] noted that there had been a 200 percent increase in DDoS attacks from 250 in 2011 to 768 in 2012. Of note is the fact that this only included attacks that required intervention by humans rather than automated defenses. According to Akamai, "Distributed Denial of Service attacks have existed since the Internet was created. In recent years, they have been gaining in popularity in large part because the technical barriers to creating such an attack are small and because it is difficult and time consuming to track an attack back to its true source." [8]. Although many of the attacks observed by Akamai were directed at the commerce industry there were 9 percent of the attacks that focused on energy and utility companies. This is significant in that these companies are representative of companies that may provide services to critical infrastructure as defined by the DoD. That said, a well-targeted DDoS attack on a financial institution might have a similar disabling effect on operations by impacting the economy rather than a military target. Akamai stated that DDoS attacks, "tend to be relatively easy to defend against, since the majority of attacks are volumetric in nature, whether SYN floods or HTTP GET floods. However, the attacks associated with Operation Ababil indicate that this won't always be the case; attackers are developing new methodologies and tools to make their DDoS efforts more effective."

In summary, the primary methods of defending

against DDoS attacks have focused on a combination of filtering, over provisioning of resources, and obscuring the location of the resources under attack via firewalls, larger bandwidth connections, and the implementation of Anycast [58]. However, as these reports show, the attackers and their methods are evolving to more sophisticated approaches which make these defenses less effective. The industry must be prepared to respond to new attacks when they occur or suffer the consequences.

9 Critical and Emerging Threats

The nature of DDoS attacks has changed significantly over the years, and this section attempts to capture some of the current critical and emerging DDoS threats. Because DDoS attacks are primarily disruptive in nature and do not typically result directly in monetary gain or permanent destruction, they can be a costly endeavor to make effective. The ultimate DDoS attack would be one that is able to take down targets at will and keep them down indefinitely with minimal effort. However, this is not typically the case, and attacks often require great amount of resources, are not persistent, and rarely cause any lasting damage. Once the attack stops or the defender is able to filter or block the attack traffic, service returns to normal. Even so, the use of botnets for political reasons, cyber extortion, or to disrupt time-sensitive operations such as stock markets have been reason enough for DDoS attacks to continue to plague the Internet, and maintain demand for botnet markets. As long as DDoS and botnets remains a viable way to make money or cause harm to adversaries, new DDoS attack methods will continue to be developed and utilized.

9.1 Continued DDoS Toolkit Development.

While DDoS toolkits such as Dirt Jumper and Pandora have been around for a while, they are continuously being upgraded by criminal organizations to utilize more refined DDoS attacks and give more flexibility to the attacker in order to customize their attacks. The most recent update (as of the publication of this paper) to the Dirt Jumper toolkit adds additional security, the ability for "turn-by-turn" attack directions, and more advanced attack mechanisms [59]. The lucrative business of renting bots can ensure that criminal organizations will attempt to continue to refine these tools to keep up with advances in DDoS defense.

9.2 N^2 Attacks

Recent research has proposed that a new category of DDoS attack may be possible that targets Internet bottlenecks without directly attacking the target, making the attack significantly more persistent and undetectable by traditional means. These attacks, termed N^2 involve bots creating relatively low volume data with decoy servers so that their network traffic will flow through target bottlenecks routers that are identified in a reconnaissance phase. Attacks proposed that utilize this strategy include the Coremelt Attack and the Crossfire attack [60] [61]. In order to carry out these attacks, reconnaissance is first performed to determine the critical routers surrounding a target. This reconnaissance can be performed using the existing botnets along with common tools such as traceroute. Once critical routers are identified, low-rate data streams can be sent either amongst bots or to decoy servers so that these streams traverse those routers. If enough flows are generated, these routers may become congested, thus restricting legitimate traffic through these routers. Because the flows generated by the bots never touch the target network, these attacks may be very difficult to detect and an advanced attacker may also be able to automatically adjust their attack to outpace Internet congestion protocols, thus generating a highly persistent DDoS attack. While overlay networks (discussed in section 9.1), information sharing amongst ISPs, or other DDoS technologies may provide potential solutions for these attacks, more research must be done to evaluate their effectiveness against N^2 attacks [61] [62].

9.3 Application Layer Attacks

Application layer attacks are becoming increasingly popular attack method in the realm of DDoS attacks, with Prolexic estimating that they made up over 75% of all DDoS attacks in the first quarter of 2013. These attacks are gaining popularity because of their ability to bring down services using a fraction of the attack data utilized in traditional attacks that target network and transport layers [41]. These attacks target protocols such as HTTP, DNS, VoIP, and SMTP, attempting to overwhelm applications servers and make them unavailable to legitimate users. One way an attacker may do this is to identify an application request type that requires significantly more work to fulfill than is required to make the request. The target application may then be overwhelmed by a large number of non-resource intensive requests that require significantly more work to fulfill [63]. Some of these attacks may even be effective from a single attacking source, but if utilized in a distributed manner may further amplify the effects of this attack or allow the attack to be sustained for a greater period of time.

Tools that may be used to perform these application layer attacks include slowloris [48], r-u-dead-yet [64], slowhttptest [65], and are easily available for download. Bot-specific malware that includes the capability of application layer attacks includes BlackEnergy and YoYoDDoS [63]. Defense from these attacks can be difficult because attack traffic may be indistinguishable from legitimate traffic, and very difficult to block if attacks are arrive from distributed source IP addresses [66]. DDoS defense providers such as Cloudflare and Arbor Networks currently provide services that attempt to filter application attack traffic, though there is still the risk that these will either miss malicious traffic, or filter legitimate traffic. During normal operations Cloudflare even states that they are only able to filter approximately 90% of application attack traffic; in order to prevent the remaining attack traffic, tradeoffs must be made that will affect access to the service or website [46].

9.4 Fully automatic DDoS attack

Since classified networks are largely separated from the rest of the Internet, it means that traditional DDoS attacks may not be effective against them. However, Mirkovic and Reiher [40] suggests the idea of a fully automatic DDoS. In a fully automatic attack, these bots could get onto the classified network using an infected USB device or other means, and then replicate as a worm across the network. At a specific time, these bots could begin sending DDoS traffic across the DoD network creating network congestion. This DDoS traffic could disrupt command and control or simply be a hindrance preventing the remote patching of machines while causing other problems, such as destroying data, or causing physical damage to equipment. [67]. Following best practices, ensuring systems are patched, and proper enforcement of physical

security all make this type of attack more difficult, but a worm using a zero-day exploit could still potentially infect and propagate through a network faster than action can be taken against it.

9.5 Other DDoS Concerns

The above threats are not all inclusive, and there will certainly be new threats and attack methods developed that have yet to be considered by researchers. Other problems, though not technical, could cause further problems as more devices are connected to the Internet. Emerging economies continue to become more connected this flood of new Internet connected devices that are at risk of becoming bots if not properly patched and maintained. The adoption of Internet Protocol Version 6 (IPV6) could present a similar problem, as ordinary, everyday devices are connected to the Internet with their own IP addresses. Other threats such as Hacktivist groups, while generally little more than a nuisance, are well organized and have a legion of dedicated followers willing to carry out DDoS attacks without the need for bots. If their tactics and capabilities improve, there is the potential that these groups could become a significant DDoS threat. Along with the known threats, there are always the unknown threats out there as nations, criminals, and other organizations continue to look for ways to make profit or cause harm to their adversaries, making it even more important to continue to research DDoS and its prevention.

10 Future research

The basic approaches to dealing with DDoS are a set of heuristics and best practices. As previously indicated the current Internet architecture makes it very difficult to solve the DDoS problem due to the lack of traceability or verification of IP source addresses and the stateless nature of the network layer. There are three primary defense methodologies, which exist to combat DDoS attacks: overlay networks, identification of the perpetrators or originating networks and distributed traffic reduction. By nature, overlay networks and distributed traffic reduction most closely align with the prevention and mitigation of the DDoS end state while identification of perpetrators is predominately reactive and attempts to stop current attacks and prevent future attacks by the identified sources.

10.1 Overlay networks

In [68], Clark et.al suggest, “Overlays may be a means to build gated communities in cyberspace.” An overlay can be thought of as a service utilized by users or applications, which ride on top of the basic existing Internet infrastructure services e.g. IP, TCP, DNS, UDP and routing protocols such as BGP. Additionally, in [68], Clark et.al provides the following definition:

> “An overlay is a set of servers deployed across the Internet that:
>
> a) Provide infrastructure to one or more applications,
>
> b) Take responsibility for the forwarding and handling of application data in ways that are different from or in competition with what is part of the basic Internet,
>
> c) Can be operated in an organized and coherent way by third parties (which may include collections of end-users) “

They also note that the beginning of the Internet was little more than an overlay, which utilized the Public Switched Telecommunications Network (PSTN) to provide the most basic of Internet capabilities. Through global adoption and dedicated infrastructure purchases, that same Internet has become the basis for newer overlay networks such as Tor, Skype and used by CDN providers like Akamai. Thus the modern day Internet will evolve through adoption and integration of these types of new overlays. As an example, the transition of global networks from IPV4 to IPV6 is a form of overlay network. Overlay network proposals such as Secure Overlay Services (SOS) [69] and OverDoSe [70] have recommended overlay network protocols capable of mitigating DDoS attacks. More recently, Scalability, Control, and Isolation On Next-Generation Networks (SCION) [71] and STRIDE [62] are proposed architectural approaches which hold promise in providing guaranteed access to users though implementations remain in the preliminary stages. The introduction of the concept of capabilities is another approach to grant access to a resource. Essentially these approaches leverage verification nodes to prioritize traffic to already authenticated requests over unauthenticated requests. Unfortunately this merely shifts the target from the actual resource to the grantor of access to the capabilities, which requires a standard datagram defense approach common to normal packet filtering [72]. Lastly, in an architectural framework proposed by Garlan et.al, Rainbow is a potential approach, which provides a self-adaptive software architecture and style to meet the dynamic changes of the network environment [73]. Currently, research is underway on the possibility of applying Rainbow to the DDoS problem.

Today, overlay networks could provide the ability to enable source routing, default disconnected states with third party approval for connections, and decoupling of names from IPs to assist in mitigating DDoS attacks. History has shown there is a constant ebb and flow in the battle for supremacy between the defenders of networks services and their attackers. There should be no doubt that whatever the solution, overlays will play a part in that defense.

10.2 Identification of attacking machines and host networks

Identification of current bots and the networks from which they originate can be both a reactive and proactive approach to DDoS attacks. In spite of the IP spoofing used by botmasters, identification of bots can be achieved through packet marking approaches. Numerous variations on this common theme exist including probabilistic and hash based marking schemes as well as packet logging. Snoeren et.al proposed a hash-based scheme, which if correctly implemented could trace back a single packet to its source [23]. Yaar et.al proposed Pi (Path Identifier) as a probabilistic approach to identify the attacker’s packets and filter them at the appropriate network point [74]. More recent approaches to identify the source of DDoS attacks utilize hybrid approaches, which combine packet marking and packet logging at intermediate points [75]. Another recent probabilistic approach, the Luby Transform Code for IP traceback (LTCIP) scheme, combines packet marking with linked lists to reconstruct attack paths in a more efficient manner [76].

Additional research in this area will likely focus on the continued reduction of the computational effort required to mark the packets or determine the origin of attack packets. This can be accomplished through optimization of the number

of packets required to generate the attack graph. Leveraging known and improved router maps can make these approaches more scalable and therefore more effective in quickly identifying the source of the attacks.

10.3 Distributed traffic reduction

Unlike the previous two approaches, distributed traffic reduction is predominantly a mitigation strategy, which seeks to minimize the impact of an ongoing attack. Early work in this area recommended explicit notification of the congestion in the network through actions by the routers. One such proposal, Random Early Detection (RED) [77], presented a construct in which detection of congestion was performed through the computation of the average queue size. When the queue length exceeds a specified number the gateway would drop a packet in order to trigger the existing TCP mechanisms on the host to throttle back the flow rate. Alternatively the router could set a congestion bit in the packet to notify the sender of the congestion. More recent implementations of this approach have been proposed. For example, Random Early Detection with Flow Trust (RED-FT) [78] uses RED with a trust mechanism which is determined both directly and probabilistically to separate legitimate flows from those of an attacker while dropping the packets from the latter. Some of the outstanding issues for these approaches are the implicit adherence to the "rules" of TCP and its lack of application to protocols, which do not implement any flow control. Another potential drawback is the requirement to add additional software and functionality to the routers.

In [79] Mahajan et.al propose aggregate based congestion control (ACC), which considers commonality of characteristics across flows such as destination or source address, application type or even protocol types such as ICMP, TCP or HTTP. This approach attempts to identify attack flows among multiple flows and types and rate limit them both locally and across the network through pushback. Similar to the aforementioned use of RED, issues with this type of approach include the requirement to install new software and the additional work required of the router at a time when the device is already overloaded.

In a patent recently awarded to Google, the use of a dedicated device, a network processor, using a specific method for detecting and filtering IP packets has been proposed to prevent DDoS attacks. The proposed method includes a bloom filter, which works in conjunction with a version of the leaky bucket algorithm to identify attack flows. The method monitors and determines a set of rules based on a set of collected indicators, which are then used to filter traffic prior to delivery to the requested resource [80].

Distributed traffic reduction requires significant change to the core of the Internet. A considerable amount of coordination across its stakeholders to properly implement these solutions would also be required. Future research in this area will likely focus on the best way to achieve the goals of DDoS mitigation with a minimal amount of change to routing software. International agreement upon the integration of the required changes into the network layer will be one of the biggest challenges for these approaches.

11 Conclusion

This paper has focused on numerous defense techniques presented within the structure of the Lockheed Martin intrusion kill chain. When applied in a layered approach, these techniques provide the best possible defense against DDoS attacks. History has demonstrated the ebb and flow of new attacks and new defenses will not soon come to an end. From our survey it is clear that the best way to defeat DDoS attacks is by preventing them. Botnets are a core enabler for the successful execution of DDoS attacks. Therefore, in conjunction with continued research to improve network layer protocols and implement new overlay approaches, a more concerted and comprehensive effort should be applied to prevention, detection and dismantling of botnets. That effort should not only include technical improvements such as modification to network protocols by removing some of the current holes but also policy approaches to address the economic factors of information security such as those discussed by Ross Anderson [81].

12 Appendix A

Definitions from the Lockheed Martin paper [3] for the stages of the "Intrusion Kill Chain" are quoted below. The intrusion kill chain is defined as reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives. With respect to computer network attack (CNA) or computer network espionage (CNE), the definitions for these kill chain phases are as follows:

1. Reconnaissance - Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.

2. Weaponization - Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.

3. Delivery - Transmission of the weapon to the targeted environment. The three most prevalent delivery vectors for weaponized payloads by APT actors, as observed by the Lockheed Martin Computer Incident Response Team (LM CIRT) for the years 2004-2010, are email attachments, websites, and USB removable media.

4. Exploitation - After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.

5. Installation - Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.

6. Command and Control (C2) - Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have \hands on the keyboard" access inside the target environment.

7. Actions on Objectives - Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration, which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.

13 Acknowledgments

Thank you to all those that provided guidance, references, discussion, and more to us during our research of this subject. Your time is valuable and we appreciate you affording some to us. Nicolas Christin and Virgil Gligor of CMU, LCDR Paige Adams and his colleagues at Naval Cyber Defense Operations Command, and Rohan Amin of Lockheed Martin deserve special thanks for their insight they provided into this topic.

13 Bibliography

[1] B. B. Gupta, R. C. Joshi and M. Misra, "Distributed Denial of Service Prevention Techniques," *International Journal of Computer and Electrical Engineering,* vol. 2, no. 2, pp. 268-276, 2010.

[2] Arbor Networks, "DDoS: From Nuisance to Menace," 1 November 2012. [Online]. Available: http://www.arbornetworks.com/corporate/blog/4676-a-decade-of-ddos. [Accessed 21 June 2013].

[3] E. M. Hutchins, M. J. Cloppert and R. M. P. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," in *Proceeding of the 6th International Conference on Information Warfare and Security*, Washington, D.C., 2011.

[4] Z. Zhu, G. Lu, Y. Chen, Z. J. Fu, P. Roberts and K. Han, "Botnet Research Survey," in *Annual IEEE International Computer Software and Applications Conference*, 2008.

[5] C. Patrikakis, M. Masikos and O. Zouraraki, "Distributed Denial of Service Attacks," *Internet Protocol Journal,* vol. 7, no. 4, pp. 13-35, December 2004.

[6] J. Nazario, "Politically Motivated Denial of Service Attacks," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, IOS Press, 2009, pp. 163-181.

[7] McAfee, "10 Days of Rain in Korea," June 2011. [Online]. Available: http://blogs.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf. [Accessed 22 June 2013].

[8] Akamai Technologies, The State of the Internet, 4th Quarter, 2012 Report, vol. 5, D. Belson, Ed., Akamai Technologies.

[9] Stop DDoS, "DDoS Attack Prevention," 28 March 2013. [Online]. Available: http://ddosattackprotection.org/a-ddos-attack-so-big-the-internet-almost-broke/. [Accessed 1 June 2013].

[10] Arbor Networks, "Worldwide Infrastructure Security Report," Arbor Networks, 2012.

[11] E. Wong, "Hackers Find China Is Land of Opportunity," 22 May 2013. [Online]. Available: http://www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html?pagewanted=all. [Accessed 1 July 2013].

[12] J. Markoff, "Before the Gunfire, Cyberattacks," 12 August 2008. [Online]. Available: http://www.nytimes.com/2008/08/13/technology/13cyber.html?em&_r=0. [Accessed 1 July 2013].

[13] C. Williams, "The Telegraph," 20 January 2012. [Online]. Available: http://www.telegraph.co.uk/technology/news/9027246/Anonymous-attacks-FBI-website-over-Megaupload-raids.html. [Accessed 25 June 2013].

[14] E. Knutsen, "INSIGHT-From remote Mauritania, hacker fights for Islam worldwide," 28 June 2013. [Online]. Available: http://www.reuters.com/article/2013/06/28/mauritania-hacker-idUSL5N0F132K20130628. [Accessed 14 July 2013].

[15] E. Chickowski, "10 Notorious Cyber Gangs," 19 August 2008. [Online]. Available: http://www.baselinemag.com/c/a/Security/10-Notorious-Cyber-Gangs. [Accessed 25 June 2013].

[16] Defense Science Board, "Resiliant Military Systems and the Advanced Cyber Threat," 2013.

[17] RSA Division of EMC, "Stalking the Kill Chain," October 2012. [Online]. Available: http://www.emc.com/collateral/hardware/solution-overview/h11154-stalking-the-kill-chain-so.pdf. [Accessed 28 May 2013].

[18] Mandiant, "Mandiant Intelligence Center Report," 18 February 2013. [Online]. Available: http://intelreport.mandiant.com/?gclid=CJewmIXj-rcCFa7m7AodXn4AVw. [Accessed 24 May 2013].

[19] Prolexic, "Prolexic Threat advisory: Pandora DDoS Toolkit," Prolexic, 2012.

[20] S. Gallagher, "A beginner's guide to building botnets—with little assembly required," 11 April 2013. [Online]. Available: http://arstechnica.com/security/2013/04/a-beginners-guide-to-building-botnets-with-little-assembly-required/1/. [Accessed 20 June 2013].

[21] Trend Micro Incorporated, "Russian Underground 101," Trend Micro, 2012.

[22] N. Hachem, Y. B. Mustapha, G. G. Granadillo and H. Debar, "Botnets: Lifecycle and taxonomy," in *Network and Information Systems Security (SAR-SSI)*, La Rochelle, 2011.

[23] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent and W. T. Strayer, "Single-Packet IP Traceback," *Networking, IEEE/ACM Transactions on (Volume:10 , Issue: 6),* pp. 721-734, 2002.

[24] A. K. Ansah, J. Kyei-Nimakoh and M. Kontoh, "Analysis of freeware hacking toolkit," *World congress on engineering and computer science,* pp. 140-149, 2012.

[25] F. Freiling, T. Holz, M. Steiner, F. Dahl and E. Biersack, *Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm,* 2008.

[26] E. Messmer, "Navy Marine Corps Intranet hit by Welchia worm," 19 August 2003. [Online]. Available:

http://www.networkworld.com/news/2003/0819navy.html. [Accessed 26 June 2013].

[27] D. Geer, R. Bace, P. Gutmann, P. Metzger, C. Pfleeger, J. Quarterman and B. Schneir, "Cyberinsecurity: The cost of monopoly," 2003.

[28] M. R. Chouchane and A. Lakhotia, "Using engine signature to detect metamorphic malware," *Proceeding,* pp. 73-78, 2006.

[29] J. M. Hagen, E. Albrechtsen and J. Hovden, "Implementation and effectiveness of organizational information security measures," *Information Management & Computer Security, Vol. 16 Iss: 4,* pp. 377-397, 2008.

[30] DISA, "Host Based Security System," 08 March 2013. [Online]. Available: http://en.wikipedia.org/wiki/Host_Based_Security_System. [Accessed 26 June 2013].

[31] H. Pareek, S. Romana and P. R. L. Eswari, "Application whitelisting: approaches and challenges," *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.5,* 2012.

[32] M. Bailey, E. Cooke, F. Jahanian, Y. Xu and M. Karir, "A Survey of Botnet Technology and Defenses," in *Cybersecurity Applications & Technology Conference For Homeland Security*, 2009.

[33] G. Gu, R. Perdisci, J. Zhang and W. Lee, "Botminer: Clustering analysis of network traffic for protocol- and structure-independent botnet detection," *Proceedings,* pp. 139-154, 2008.

[34] J. C. Mitchell and E. Stinson, "Characterizing bots' remote control behavior," Stanford University, 2007.

[35] H. Zeidanloo, M. Shooshtari, P. Amoli, M. Safari and M. Zamani, "A taxonomy of botnet detection techniques," in *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on (Volume:2)*, 2010.

[36] T. Ormerod, *AN ANALYSIS OF A BOTNET TOOLKIT AND A DEFAMATION ATTACK,* Montreal, Quebec: Concordia University, 2012.

[37] R. Lemos, "Microsoft, FBI Shutter Citadel Botnets Seeking to End $500M Crime Spree," 6 June 2013. [Online]. Available: http://www.eweek.com/security/microsoft-fbi-shutter-citadel-botnets-seeking-to-end-500m-crime-spree/. [Accessed 27 June 2013].

[38] P. Bright, "How Operation b107 decapitated the Rustock botnet," 22 March 2011. [Online]. Available: http://arstechnica.com/information-technology/2011/03/how-operation-b107-decapitated-the-rustock-botnet/. [Accessed 27 June 2013].

[39] P. Martin, "Obama's "Cyberwarfare First Strike": Using Offensive Cyber Effects Operations (OCEO) to Destabilize Countries," 10 June 2013. [Online]. Available: http://www.globalresearch.ca/obamas-cyberwarfare-first-strike-using-offensive-cyber-effects-operations-oceo-to-destabilize-countries/5338457. [Accessed 27 June 2013].

[40] J. Mirkovic and P. Reiher, A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, vol. 34, ACM SIGCOMM Computer Communications Review, 2004, pp. 39-53.

[41] S. McClure, J. Scambray and G. Kurtz, Hacking Exposed 7, McGraw-Hill, 2012.

[42] Fyodor, "Nmap - Free Security Scanner For Network Exploration & Security Audits," [Online]. Available: nmap.org. [Accessed 5 7 2013].

[43] Carnegie Mellon CERT, "CERT Advisory CA-1997-28 IP Denial-of-Service Attacks," 16 12 1997. [Online]. Available: https://www.cert.org/advisories/CA-1997-28.html. [Accessed 17 07 2013].

[44] A. Kuzmanovic and E. W. Knightly, "Low-Rate TCP-Targeted Denial of Service Attacks," in *SIGCOMM*, Karlsruhe, 2003.

[45] F. Gont, *ICMP Attacks against TCP,* Internet Engineering Task Force, 2010.

[46] Cloudflare, "CloudFlare advanced DDoS protection," 2013. [Online]. Available: www.cloudflare.com/ddos. [Accessed 08 07 2013].

[47] Radware, "DDoSS Survival Handbook," Radware, Ltd., 2013.

[48] RSnake, "Slowloris HTTP DoS," June 2009. [Online]. Available: http://ha.ckers.org/slowloris/. [Accessed 08 July 2013].

[49] M. Marquez Andrade and N. Vlajic, Dirt Jumper: A New and Fast Evolving Botnet-for-DDoS, vol. 3, Toronto, Ontario: International Journal of Intelligent Computing Research (IJICR), 2012, pp. 330-336.

[50] T. Peng, C. Leckie and K. Ramamohanarao, "Survey of Network-Based Defense Mechanisms Counter the DoS and DDoS Problems," *ACM Computing Surveys,* vol. 39, no. 1, April 2007.

[51] M. H. Bhuyan, H. Kashyap, D. Bhattacharyya and J. Kalita, "Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions," *The Computer Journal,* 2013.

[52] S. Agarwal, T. Dawson and C. Tryfonas, "DDoS Mitigation via Regional Cleaning Centers," Sprint ATL Research Report, 2004.

[53] Prolexic, "The best on-demand, cloud-based scrubbing centers for DDoS protection," [Online]. Available: https://www.prolexic.com/why-prolexic-best-dos-and-ddos-scrubbing-centers.html. [Accessed 10 July 2013].

[54] AT&T, "AT&T DDoS Protection," AT&T, [Online]. Available: http://www.business.att.com/enterprise/Service/network-security/threat-vulnerability-management/ddos-

protection/. [Accessed 10 July 2013].

[55] Verisign, "DDoS Protection Services," Verisign, [Online]. Available: https://www.verisigninc.com/en_US/products-and-services/network-intelligence-availability/ddos/mitigation-services/index.xhtml. [Accessed 10 July 2013].

[56] Arbor Networks, "Cloud Signaling Coalition (CSC)," 2012. [Online]. Available: http://www.arbornetworks.com/products/cloud-signaling-coalition. [Accessed 10 July 2013].

[57] Prolexic Technologies, "Prolexic Quarterly Global DDoS Attack Report Q1 2013," 2013.

[58] M. Prince, "Evil DoS Attacks and Strong Defenses," in *DefCon*, Las Vegas, 2013.

[59] J. Jones, "DirtJumper's DDoS Engine Gets a Tune-Up with new "Drive" Variant," Arbor Networks, 20 June 2013. [Online]. Available: http://ddos.arbornetworks.com/2013/06/dirtjumpers-ddos-engine-gets-a-tune-up-with-new-drive-variant/ . [Accessed 4 July 2013].

[60] A. Struder and A. Perrig, "The Coremelt Attack," in *ESORICS*, 2009.

[61] M. S. Kang, S. B. Lee and V. D. Gligor, "The Crossfire Attack," in *IEEE Symposium on Security and Privacy*, 2013.

[62] H.-C. Hsiao, H. Hyun-Jin Kim, S. Yoo, X. Zhang, S. B. Lee, V. Gligor and A. Perrig, "Sanctuary Trail: Refuge from Internet DDoS Entrapment," 7 June 2012. [Online]. Available: http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12013.pdf. [Accessed 26 May 2013].

[63] Arbor Networks, "The Growing Threat of Application-Layer DDoS Attacks," Arbor Networks, 2012.

[64] "r-u-dead-yet," 2011. [Online]. Available: https://code.google.com/p/r-u-dead-yet/. [Accessed 17 07 2013].

[65] "slowhttptest," 2012. [Online]. Available: https://code.google.com/p/slowhttptest/. [Accessed 17 07 2013].

[66] Y. Xie and S.-Z. Yu, "A novel Model for Detecting Application Layer DDoS Attacks," *Proceedings of IMSCCS '06,* 2006.

[67] N. Weaver and V. Paxson, A Worst-Case Worm, Third Annual Workshop on Economics and Information Security , 2004.

[68] D. CLARK, B. LEHR, S. BAUER, P. FARATIN, R. SAMI and J. WROCLAWSKI, "Overlay networks and the future of the internet," *COMMUNICATIONS & STRATEGIES, no. 63, 3rd quarter,* pp. 1-20, 2006.

[69] A. D. Keromytis, V. Misra and D. Rubenstein, "SOS: Secure overlay services," in *SIGCOMM '02*, Pittsburgh, 2002.

[70] E. Shi, I. Stoica, A. David and A. Perrig, "Overdose: A generic ddos protection service using an overlay network," CMU, Pittsburgh, 2006.

[71] X. Zhang, H.-C. Hsiao, G. Hasker, H. Chan, A. Perrig and A. D. G, "SCION: Scalability, control, and isolation on next-generation networks," in *Security and Privacy (SP), 2011 IEEE Symposium on*, 2011.

[72] K. Argyraki and D. R. Cheriton, "Network Capabilities: The Good, the Bad and the Ugly," *Hotnets,* p. November, 2005.

[73] D. Garlan, B. Schmerl and S.-W. Cheng, "Software Architecture-Based Self-Adaptation," *Autonomic Computing and Networking,* pp. 31-55, 2009.

[74] D. Yaar, A. Perrig and A. Song, "Pi: a path identification mechanism to defend against DDoS attacks," in *Symposium on Security and Privacy*, 2003.

[75] M.-H. Yang and M.-C. Yang, "RIHT: A Novel Hybrid IP Traceback Scheme," *Information Forensics and Security, IEEE Transactions on (Volume:7 , Issue: 2) ,* pp. 789-797, 2012.

[76] S.-H. Peng, K.-D. Chang, J.-L. Chen, I.-L. Lin and H.-C. Chao, "A Probabilistic Packet Marking scheme with LT Code for IP Traceback," *International Journal of Future Computer and Communication,* 2012.

[77] S. Floyd and V. Jacobson, "Random early detection gateways for congestion avoidance," *IEEE/ATM Transactions on networking,* pp. 397-413, 1993.

[78] X. Jiang, J. Yang, G. Jin and W. Wei, "RED-FT: A Scalable Random Early Detection Scheme with Flow Trust against DoS Attacks," *Communications Letters, IEEE (Volume:17 , Issue: 5) ,* pp. 1032-1035, 11 March 2013.

[79] R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson and S. Shenker, "Controlling High Bandwidth Aggregates in the Network," *ACM SIGCOMM Computer Communication Review Volume 32 Issue 3,* pp. 62-73, July 2002.

[80] M. C. Chuah, W. C. Lau and O.-C. Yue.United States of America Patent US8201252 B2, 2012.

[81] R. Anderson, "Why Information Security is Hard-An Economic Perspective," in *ACSAC '01 Proceedings of the 17th Annual Computer Security Applications Conference*, 2001.