CHAPTER 3

REVIEW OF SOLUTIONS FOR DDoS ATTACKS ON CLOUDS

3.1 ABSTRACT

Internet has become the key driver for an organization’s growth, brand awareness and operational efficiency. Unfortunately, cyber terrorists and organized criminals recognize this fact as well. Using Distributed Denial of Service (DDoS) attacks cyber criminals deny the legitimate users the access to the hosted services, by causing web sites to perform slowly and deny access to corporate network and data. This chapter illustrates the current trends and threats posed by cyber-attacks and presents results of the DDoS Survey conducted by the Researcher for cyber threats and attacks faced by organizations and Cloud service providers. This chapter reviews DDoS mitigation strategies for different types of distributed denial of service attacks and also examines the existing DDoS solutions available for Cloud environments.

3.2 CYBER ATTACK TRENDS

The Researcher initially reviewed Cyber Security Attack & DDoS reports from Imperva (2016) and Akamai State of Security (2015) among other cyber security reports. Following are the primary trends seen for DDoS attacks in 2016.

- Large Botnets – there is a steady increase in the intruder abilities for deploying large sized attacks with a 73% increase in peak attack size (579Gbps) over 2015, 274 attacks over 100Gbps and 46 attacks over 200Gbps monitored in 2016, versus 223 in 2015 and 16 in all of 2016 (Imperva and Akamai DDoS 2015-16 reports).

- Advanced Zombie attacks – 75% organizations reported existing BOT infections, attack vectors include Heap-based buffer overflow vulnerability on Linux servers, use of Microsoft SQL Reflection techniques and 45% of Cloud based SaaS industries are being targeted (as per Imperva and Akamai DDoS 2015-16 reports).

- Attack Frequency – there was an average of 124,000 events per week over the last 18 months with USA, France and Great Britain being the top targets for attacks over 10Gbps (as per Imperva and Akamai DDoS 2015-16 reports).

Impact – 82% of organizations reported employees accessed sites found to be malicious, 92% of organizations downloaded a malicious payload file while 88% organizations suffered data loss and 400% increase in loss of business (as per Imperva and Akamai DDoS 2015-16 reports).

The recent attacks are hard to defend using standard techniques as the malicious DDoS requests differ from legitimate requests only in intent, and not in content.

3.3 CYBER SECURITY SURVEY

An electronic survey was conducted from 15th January 2014 to 15th March 2014 with the focus on cyber-attack threats and the impact on organizations. Using Survey Monkey as the contact medium questionnaire requests were sent to 700 IT security and industry professionals with responses received from 550 participants.

In order to ensure the survey had the right mix of target audience –

- The Researcher ensured the industry representation of respondents involved Information Technology professionals from Cloud Computing, Information Security, Data Center and Infrastructure Operations domains.

- The Researcher also ensured the respondents belonged to a broad range of industries across different organizations with more than 1000 employees

- The survey requests sent were evenly divided among domestic and international respondents with global locations and businesses utilizing Cloud Computing.

Detailed breakup, roles and responsibilities are presented in Tables 3.1 and 3.2 below.

Respondent's Roles	Breakup
Information Security	33%
Security Operations	18%
Network Security	12%
IT Support	9%
Systems Admin	8%
Audit Compliance	7%
Web Deployment	6%
Data Center Ops	7%

Table 3.1. Respondents Roles

Organization	Count	Breakup
Financial Services	66	12%
Education	05	1%
Information Technology	245	45%
Retail, E-commerce	45	8%
Internet Service Providers	44	8%
Gaming	105	19%
Media & Travel	30	5%
Pharmacy	10	2%

Table 3.2. Respondent Organizations

Respondent's views and results of the survey are as illustrated below.

Survey Question #1: In case of DDoS attack whose responsibility is established for incident response and attack mitigation?

While there is no one team dedicated to mitigate cyber-attacks, most organizations deploy a team from the Network and Information Security domains from within the organization to work together with shared responsibility during a DDoS attack till the DDoS has been mitigated, in other words a combined team drives the mitigation plan, as illustrated in Figure 3.1.

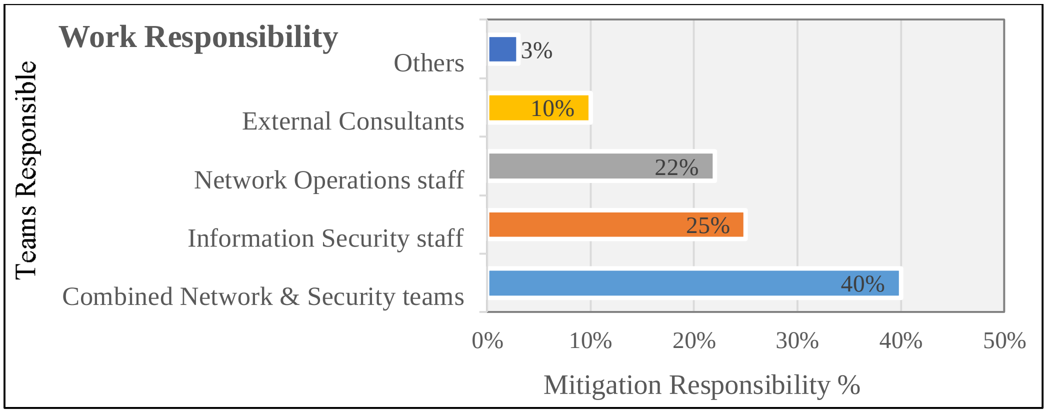

Figure 3.1: Respondents work responsibilities

Survey Question #2: What factors are accounted to weigh the impact of DDoS attack in the organization?

Commercial impact and high cost of technical repairs and support involved are the top two issues concerning organizations regarding the impact of a DDoS attack on the organization as illustrated in Figure 3.2.

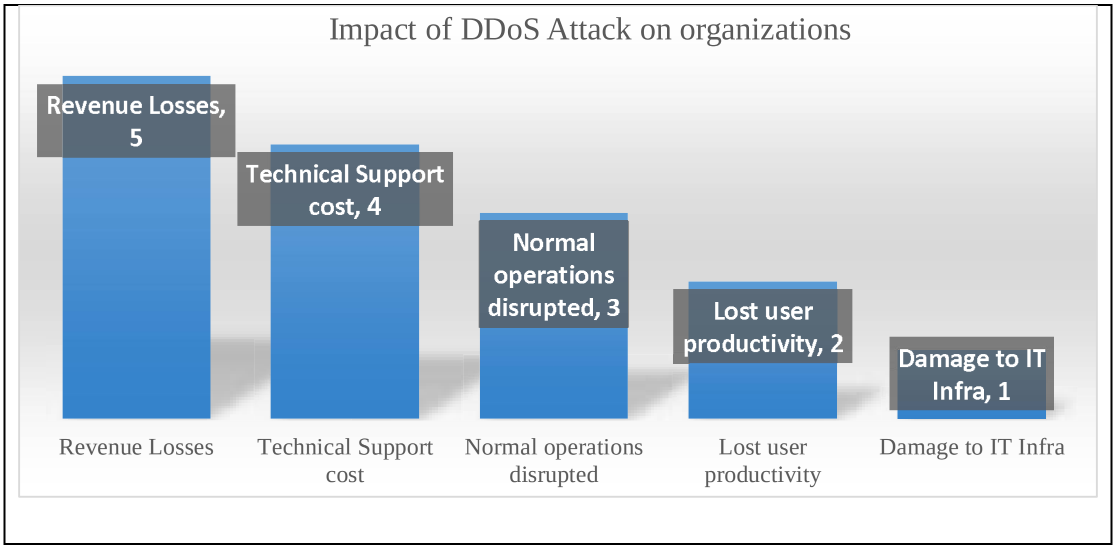

Figure 3.2: Impact of DDoS Attack on organizations

Survey Question #3: Does your organization have the ability to block and prevent DDoS attacks?

Ideally every organization should have a mitigation plan ready but only 54% organization felt confident enough to confirm the ability to block and contain a DDoS attack. This is presented in Figure 3.3 below. This assumption however is largely untested as most organizations only assume their ability and don't have a valid test result to prove the plan.

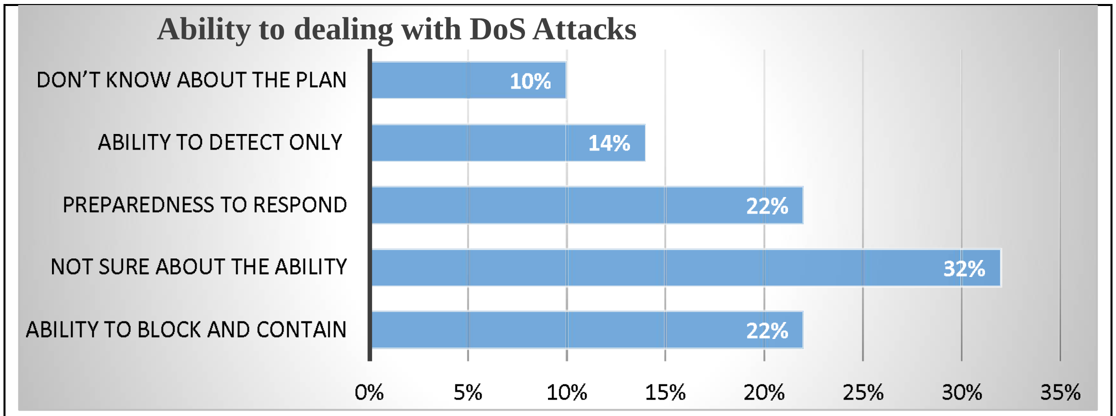

Figure 3.3: Ability to deal with DDoS Attacks

Survey Question #4: Please rate and categorize the impact areas as a result of DDoS attack?

Loss of trust with lower customer confidence is one of the most damaging consequences of DDoS attacks as the business takes a huge hit as presented in Figure 3.4.

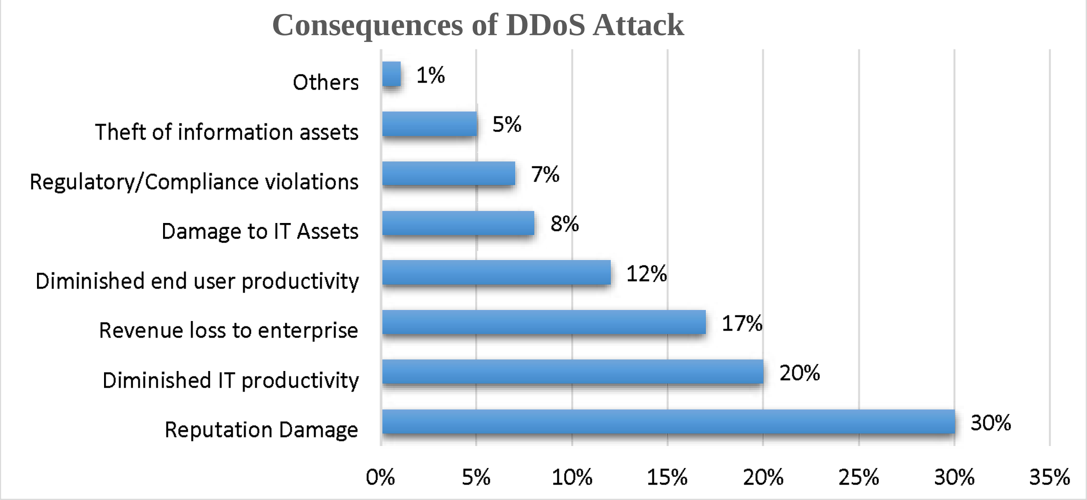

Figure 3.4: Consequences of DDoS Attacks

Survey Question #5: What are the barriers that prevent DDoS mitigation implementation?

Lack of budget and knowledge skills are the top obstacles which prevent DDoS mitigation implementations for the organizations as shown in Figure 3.5.

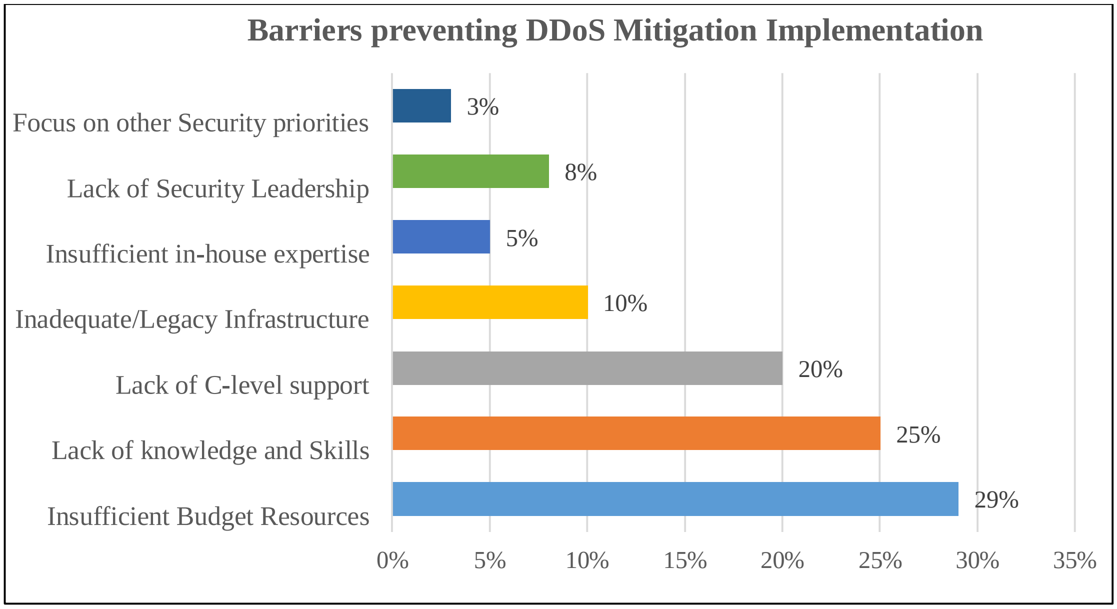

Figure 3.5: Barriers preventing DDoS Mitigation Implementation

Survey Question #6: Which type of attacks resulted in the maximum downtime for your Cloud hosted services?

DDoS and Malware are the top ranked cyber threats for most organizations worldwide as illustrated in Figure 3.6 below.

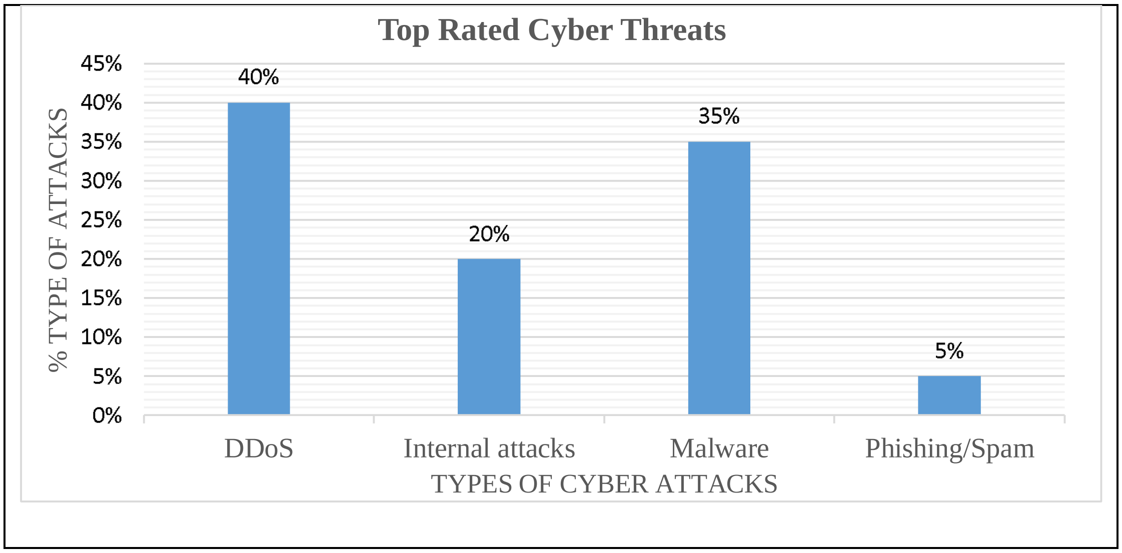

Figure 3.6: Top Rated Cyber Threats

Survey Question #7: Has a DDoS attack ever resulted in downtime of your Data center?

Unplanned Data center outages primarily due to DDoS resulted in 45% respondents confirming entire data center operations were shut down as illustrated in Figure 3.7.

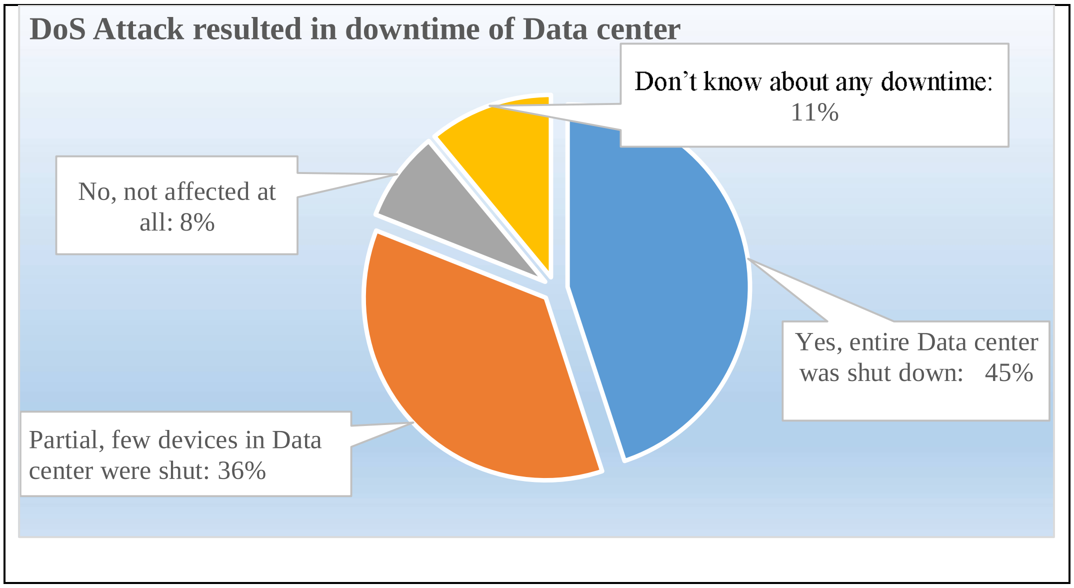

Figure 3.7: Downtime resulted due to DDoS Attacks

Survey Question #8: How often is the Enterprise Security Resilience against DDoS attacks checked in your Data center?

Majority of organizations (72%) recognize the need to have the security assessment at least once, while 49% performed the checks more than once annually. This overall is a good trend as it points to organizations taking notice of the cyber-attacks and seeking to be prepared against them is presented in Figure 3.8.

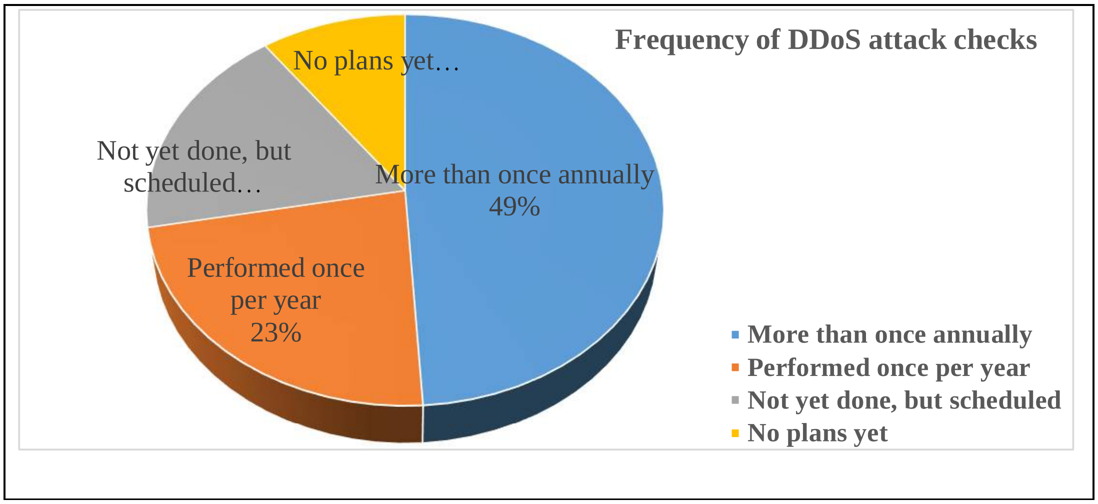

Figure 3.8: Frequency of DDoS checks performed

Survey Question # 9: How are the mitigation capabilities activated during DDoS attacks?

Organizations still rely on service providers to block DDoS on WAN circuits or the on premise deployments during DDoS attacks as presented in Figure 3.9 below.

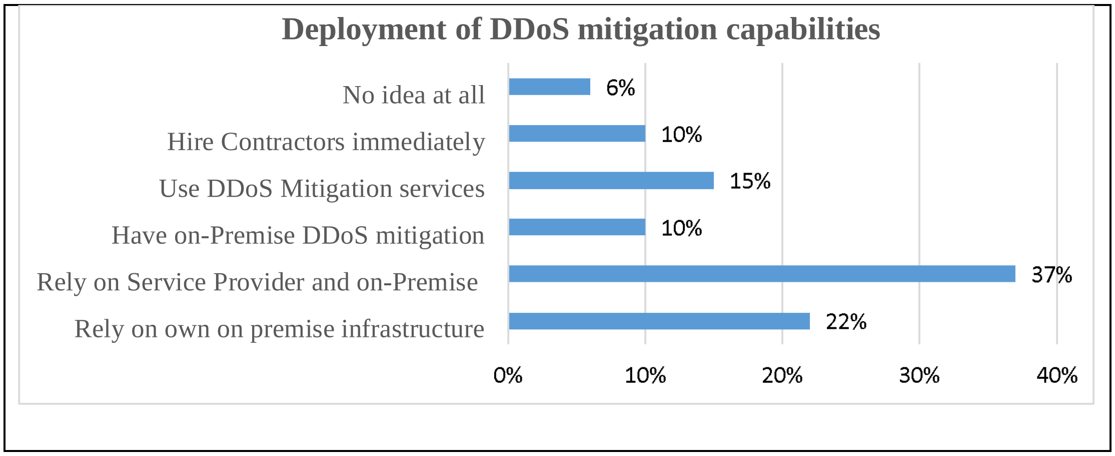

Figure 3.9: Mitigation activities during DDoS attacks

Survey Question #10: Which factors are most important during the DDoS attack?

The ability to detect DDoS attacks with as little human intervention and the reporting around the cyber-attack with visibility are the most critical factors which an organization needs to have in place as illustrated in Figure 3.10.

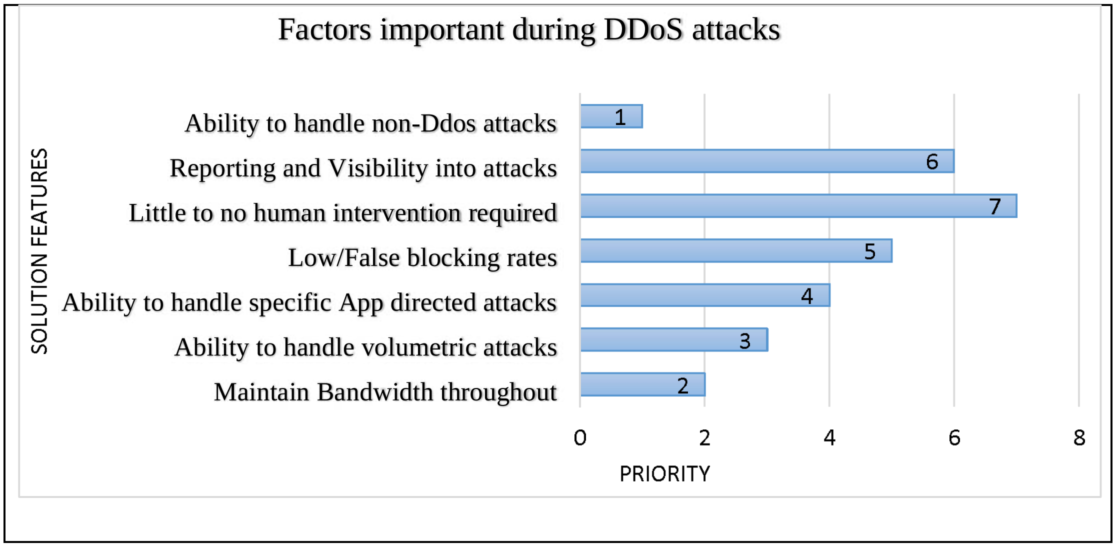

Figure 3.10: Factors important during DDoS attacks

The above survey results indicate that Security decisions are driven by Security Management and majority of the organizations have little or no idea about the actual impact of DDoS attacks. Losing trust and confidence of customers is the most damaging consequence. This leads to greater losses and technical support issues. In fact just 54% reported being confident enough to block cyber-attacks. Overall DDoS attacks and Malware are the top ranked cyber threats for all the organizations across industries.

3.4 DDoS MITIGATION STRATEGIES

DDoS mitigation needs to be seamless and comprehensive in order to protect the Cloud services and web hosting against the DDoS attacks which are aimed at different layers of the TCP stack as described by Khadke, et al. (2016) and illustrated in Figure 3.11 below. There is a need to address each type of DDoS with a unique toolset and defense strategy. The section below presents the mitigation strategies for DDoS attacks.

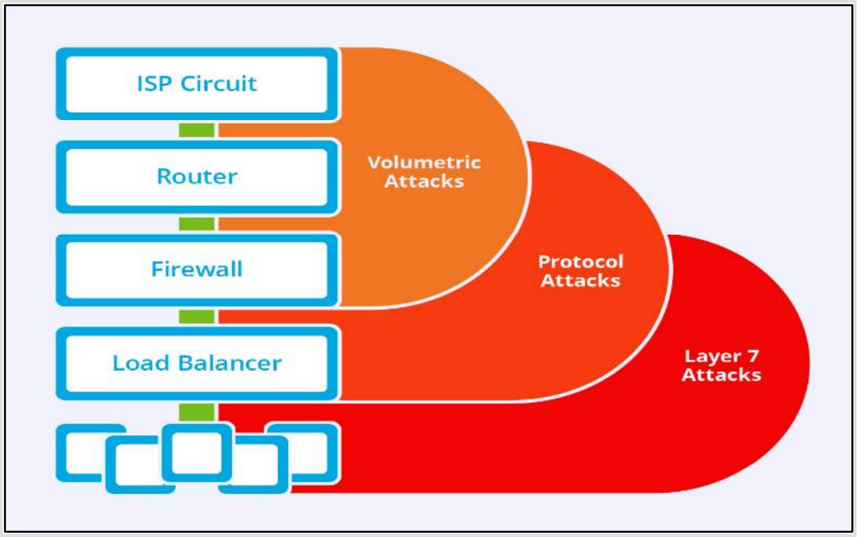

Figure 3.11: DDoS Attacks on Data Center devices (Imperva 2016 report)

3.4.1 VOLUMETRIC DDoS ATTACKS

Volumetric attacks typically impact Network Layer 4 devices while Protocol attacks occur on load balancers and firewalls. The application layer attacks occur on layer 7 server systems. Volumetric DDoS attacks as described by Geva, et al. (2014) are possible due to the relatively small network capacity of a target compared to the overall capacity of all Internet connected devices. Volumetric DDoS Mitigation Strategies range from:

- Blocking Upstream by the ISP - If contacted, the technical support arm of most ISPs will add simple rules to block specific traffic before it reaches the target network. This approach can be effective at mitigating simplistic attacks, but will often be unable to mitigate more complex scenarios. The limitation is related to the minimal filtering capabilities offered by most ISPs. For example, as illustrated in Figure 3.12 below, most ISPs will be happy to filter all traffic to or from a specific IP address, or using a certain protocol. But this is a very crude method, which may not be granular enough to block DDoS traffic and at the same time allow legitimate traffic.

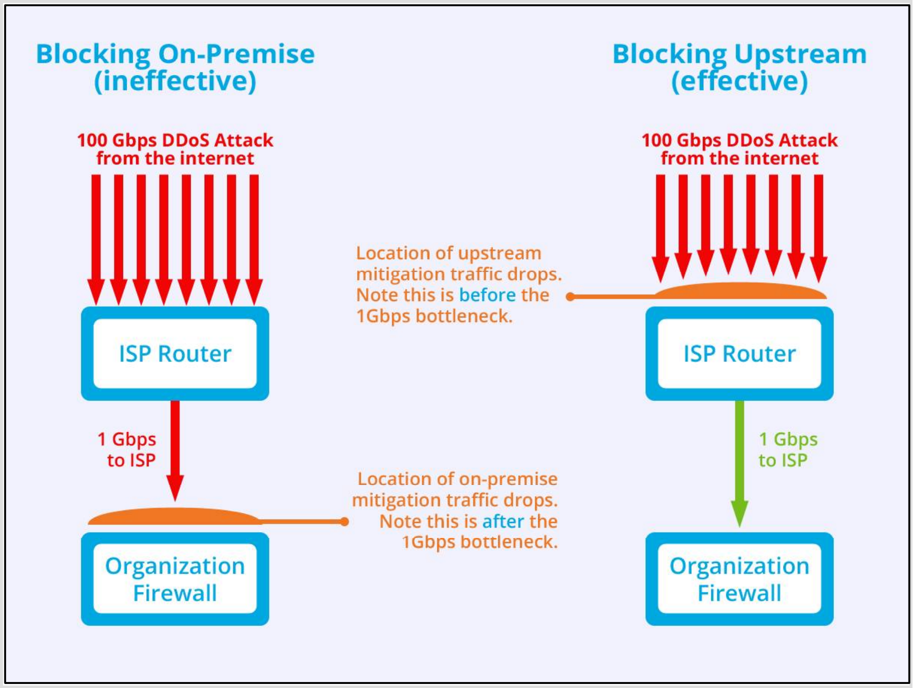
Blocking On-Premise
(ineffective)
Blocking Upstream
(effective)
100 Gbps DDoS Attack from the internet
100 Gbps DDoS Attack from the internet
Location of upstream mitigation traffic drops. Note this is before the 1Gbps bottleneck.
ISP Router
ISP Router
1 Gbps to ISP
1 Gbps to ISP
Location of on-premise mitigation traffic drops. Note this is after the 1Gbps bottleneck.
Organization Firewall
Organization Firewall

Figure 3.12: Traffic blocking by ISP (Imperva 2016 report)

- Blocking With On-Premises Devices - Attempting to block a volumetric DDoS attack using on-premises devices such as IPS/IDS and firewalls are typically ineffective. As these devices are positioned in the network downstream from the point at which the DDoS traffic causes saturation of the link and packet loss.

- Null Routing the Target IP - An organization using Border Gateway Protocol (BGP) may use null routes to prevent devices on the Internet from sending traffic to the target IP. The main benefit of this approach is its distributed effect, as the null route announcement is sent to all devices on the Internet that receive Internet routing table announcements. Since this mechanism results in the target IP becoming unreachable, it is only useful if the target IP is expendable and traffic can be discarded to save other resources on the same network. For this reason, null routes are typically only an effective mitigation in multi-user environments where a problematic user can be segmented off to ensure availability for the remaining users.

- Hide Behind a Large CDN - Traditional content distribution networks (CDNs) function by locating web server caches throughout the world to deliver content to the Internet. A CDN typically works as an HTTP(S) proxy where all requests are made to the CDN server, which subsequently initiates a private connection to the organization's server to obtain the data. With regard to volumetric attacks, using a CDN often implicitly protects a network from these types of attacks because the traffic is sent to the CDN which often is comprised of a massive, globally distributed network.

- Dedicated Mitigation Services - A dedicated DDoS mitigation service is often the most effective approach. These services are similar to the CDN approach mentioned earlier, but with advanced capabilities specific to identifying and blocking DDoS traffic. Much like a CDN, reputable mitigation services have a massive globally distributed network of scrubbing centers capable of blocking large DDoS attacks.

3.4.2 PROTOCOL DDoS ATTACKS

Unlike Volumetric attacks, the Protocol DDoS attacks intention is not to saturate the Internet connection but to cause disruption with a relatively small amount of network traffic. Protocol DDoS Mitigation Strategies range from the following.

- Blocking with On-Premises Devices - Blocking protocol DDoS attacks with on-premises devices such as IDS/IPS and firewalls may be successful due to the low bandwidth nature of these attacks. This is in contrast to volumetric DDoS attacks where the bottleneck is upstream and outside the control of the organization. Also, unlike volumetric attacks, a large portion of protocol attacks do not have spoofed source IP addresses. As a result, simple attacks can be blocked with simple firewall rules. More advanced attacks, particularly those sourced from very large botnets, will require purpose-built DDoS mitigation hardware to properly identify and automatically block the attack traffic.

- Blocking Upstream by the ISP - This method of mitigation is often ineffective for protocol DDoS attacks. If contacted, the technical support arm of most ISPs will add simple rules to block specific traffic before it reaches the target network. This approach can be effective at mitigating simplistic attacks, but will often be unable to mitigate more complex scenarios. The limitation is related to the minimal filtering capabilities offered by most ISPs. For example, most ISPs will be happy to filter all traffic to or from a specific IP address, or all traffic using a certain protocol. But this is a very blunt tool and may not be granular enough to block DDoS traffic while at the same time allowing legitimate traffic. The same level of filtering is available in on-premises firewalls and routers with the added benefit of being under the control of the organization.

- Traffic Analytics - Due to the low bandwidth nature of most protocol attacks, one of the greatest challenges is identifying that an attack is actually underway. Tools that analyze traffic patterns and look for anomalies based on historical data can be invaluable in making this determination.

- Hide Behind a Large CDN - Traditional content delivery networks (CDNs) function by locating web server caches throughout the world to deliver content to the Internet. A CDN typically works as an HTTP(s) proxy where all requests are made to the CDN server, which subsequently initiates a private connection to the organization's server to obtain the data. With regard to protocol attacks, using a CDN often implicitly protects a network from these types of attacks because the traffic is sent to the CDN which often is comprised of a massive, globally distributed network. This type of mitigation solution will only protect services supported by the CDN (generally HTTP and HTTPS).

- Null Routing the Target IP - This method of mitigation is generally not recommended for protocol DDoS attacks as it blocks all traffic to the target. This option is imprecise and will affect both legitimate and attack traffic destined for the target IP.

- Dedicated Mitigation Services - A dedicated DDoS mitigation service is often the most effective. These services are similar to the CDN approach mentioned earlier but with advanced capabilities specific to identifying and blocking DDoS traffic. Much like a CDN, a reputable mitigation service has a massive globally distributed network of scrubbing centers capable of blocking large DDoS attacks.

3.4.3 APPLICATION LAYER DDoS ATTACKS

The key differentiator between application-level and other attacks is that the attack traffic is ‘in protocol’ meaning that the traffic is legitimate from a protocol perspective. By being in protocol, the attacks are often difficult to distinguish from legitimate traffic as described by Durcekova, et al. (2012). Application DDoS attack Mitigation Strategies range from the following:

- Blocking with On-Premises Devices - Blocking application-level DDoS attacks with on-premises devices such as IDP/IPS and firewalls may be successful due to the low bandwidth nature of these attacks. This is in contrast to volumetric DDoS attacks where the bottleneck is upstream and outside the control of the organization. Unlike Volumetric or Protocol attacks, nearly all (TCP specifically) application-level attacks do not have spoofed source IP addresses. As a result, simple attacks can be blocked with simple firewall rules. More advanced attacks, and those sourced from very large botnets, will require purpose-built DDoS mitigation hardware to properly identify and automatically block the attack traffic.

- Blocking Upstream by the ISP - This method of mitigation is often ineffective for application level DDoS attacks. If contacted, the technical support arm of most ISPs will add simple rules to block specific traffic before it reaches the target network. This approach can be effective at mitigating simplistic attacks, but will often be unable to mitigate more complex scenarios. The limitation is related to the minimal filtering capabilities offered by most ISPs. For example, most ISPs will be happy to filter all traffic to or from a specific IP address, or all traffic using a certain protocol. But this is a very blunt tool and may not be granular enough to block DDoS traffic while at the same time allowing legitimate traffic. The same level of filtering is available in on-premises firewalls and routers with the added benefit of being under the control of the organization. In addition, unless they are given decryption keys, the ISP is unable to inspect the content of traffic using encrypted protocols like HTTPS, making identification and mitigation more difficult.

- Traffic Analytics - Due to the low bandwidth nature of most application-level attacks, one of the greatest challenges is identifying that an attack is actually occurring. Tools that analyze traffic patterns and look for anomalies based on historical data can be invaluable in making this determination.

- Null Routing the Target IP - This method of mitigation is generally not recommended for application-level DDoS attacks as it blocks all traffic to the target. This option is imprecise and will affect both legitimate and attack traffic destined for the target IP

- Hide Behind a Large CDN – Traditional content delivery networks (CDNs) function by locating web server caches throughout the world to deliver content to the Internet. A CDN typically works as an HTTP(s) proxy where all requests are made to the CDN server, which subsequently initiates a private connection to the organization's server to obtain the data.

- With regard to application-level attacks, using a CDN may help mitigate some attacks. Specifically, requests for resources located on the CDN, such as static web objects, will be fulfilled and absorbed by the massive CDN infrastructure.

- However, dynamic content such as user login requests, content searches or similar non-cacheable data, will be passed by the CDN to the organization's backend servers resulting in a DDoS attack. Moreover, this type of mitigation solution will only protect services supported by the CDN (generally HTTP and HTTPS).

- Dedicated Mitigation Services - A dedicated DDoS mitigation service is often the most effective approach to solving application-level attacks. These services are similar to the CDN approach mentioned earlier, but with advanced capabilities specific to identifying and blocking DDoS traffic. Much like a CDN, a reputable mitigation service has a massive globally distributed network of scrubbing centers capable of blocking large DDoS attacks.

- Application Blocking - For smaller application-level attacks, an organization may be able to mitigate the attack by disabling the feature being targeted. For example, if the attacker is targeting a search feature on the site that is inefficient, it may be better to temporarily disable that feature to maintain a proper level of performance for the other components on site.

3.4.4 REFLECTION ATTACKS

Reflection attacks are amplification attacks similar to volumetric DDoS attacks using the same protocol in both directions. Server responses sent to the source are substantially greater than the requests. Attackers take advantage of such a scenario and direct the response traffic by magnifying and flooding the victim with unwanted traffic that overwhelms the network circuits and servers. ICMP Smurf attacks on publically accessible UDP systems are examples of such attacks. Attackers send the spoofed request (64 byte) which reaches an Open Resolver Server and is then reflected to the Victim as 3,876 bytes.

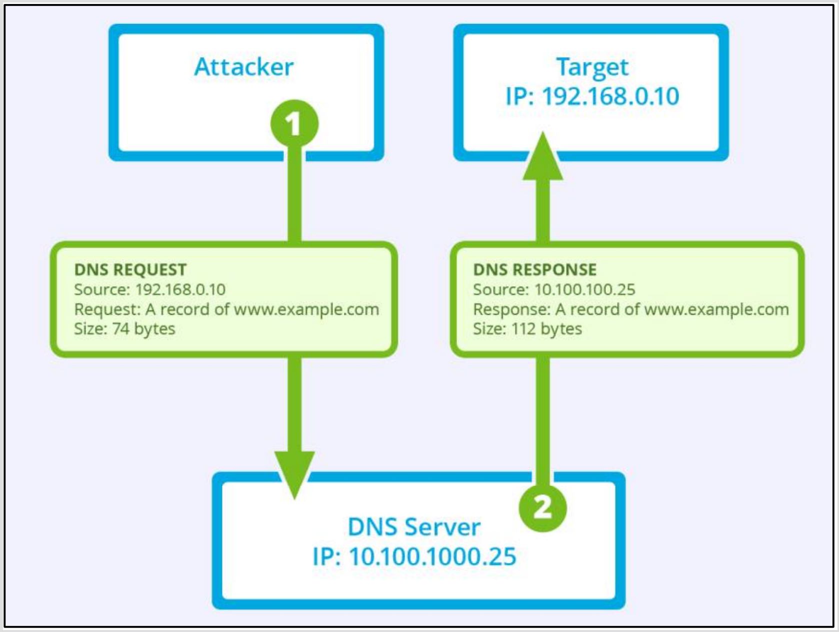

Figure 3.13: Reflection DDoS Attack process (Imperva 2016 report)

The mitigation option is to use BCP38 which allows network routers to validate IP addresses in case the attackers try to spoof the IP address, the DNS server can block reflecting traffic to the victim and only packets originating from valid IP addresses would be replied back. The notion of amplification is presented by Georgios, et al. (2007) for the DNS Reflection attack as illustrated in Figure 3.13 above. 72 byte queries like RRSIG and DNSKEY to an open vulnerable DNS resolver server results in 112 byte response.

3.5 REVIEW OF DDoS MITIGATION SOLUTIONS

Distributed Denial of Service attacks on Cloud Services has become the main threat and increased multifold in their complexity, flooding volumetric traffic, corporate enterprises, banking, financial and web hosting companies have realized the critical need to mitigate DDoS attacks. Some use ISP service offerings or use customized in-house on-premises systems, which can at best deflect a one specific type of DDoS attack or need to be constantly upgraded and customized to mitigate other types of DDoS attacks. In all, most DDoS mitigation solutions as shown by Sridaran et al. (2016) are unable to provide a proper and adequate protection against varied levels of network or application attacks, and always seem to lack the features to mitigate and block the new types of attacks that are constantly evolving. To provide a solid DDoS protection, a robust, secure and scalable solution is required. This section presents the traditional solutions for mitigating DDoS attacks.

3.5.1 ON-PREMISE DDoS MITIGATION SOLUTIONS

On premise infrastructure such as a Private Cloud with limited ISP leased bandwidth, basic security devices as firewalls and IDS proposed by Hildmann, et al. (2014). Even though an in house On-premise defense system may have DDoS mitigation defense functionalities, however it would not be able to truly deliver a proper DDoS mitigation due to the following.

- The inability of in-house defense systems in defending against volumetric floods – when attacks flood and saturate the ISP WAN circuits and the enterprise defense network themselves, becomes it a challenge to stop high-volumetric attacks on the networks.

- Another issue is the constant need for an ongoing investment on IT infrastructure, training, and resources in order to keep up with the ever increasingly dynamic DDoS threats. Most enterprises using Cloud services would not want to have an internal IT or dedicated Security groups or invest additional redundant resources.

3.5.2 ISP DDoS MITIGATION SOLUTIONS

While ISPs do tend to offer DDOS mitigation as an additional service, blocking DDoS attacks at ISP level does have drawbacks.

- With multiple customers sharing the same WAN link and the ISP providing the DDoS Service solutions using common equipment during an attack, the ISP would face issues with Internet traffic for each and every ‘protected’ customer. During the DDoS attack on one specific customer, the ISPs WAN equipment would be galvanized to handle the increased traffic flood which would in turn affect other customers who are not targeted.

- Having multiple customers with hundreds of policies to implement like blocking IP addresses, black listing domains, allow/deny ports to avoid any false positives, ISPs would at times lower their guard by 'softening' their policies and lower the alert thresholds. This can result in some malicious traffic getting passed through which even if is not a flood attack; it could lead to application attack. At times, the attacker traffic ends up behaving in a similar manner to a legitimate user's traffic request, thus leading to the ISP not being able to protect against dual network and application DDoS attack.

- ISPs core business area is network data delivery and is focused on providing WAN circuit uptimes and load balancing, expecting decent DDoS expertise would be asking a lot from network equipment vendors and they lack the required expertise to quickly respond to new types of attacks and add new attack signatures.

- Then there's the cost consideration for organizations having multiple ISPs who may have implemented BGP or WAN load balancing circuits for which implementing a DDoS protection service would require additional services to be taken from each WAN provider.

3.5.3 SCRUBBING DEFENSE DDoS MITIGATION SOLUTIONS

Use of scrubbing defense architecture is performed in two ways for DDoS protection as described by Zilberman, et al. (2015). Either ways have all the traffic go through a third party defense systems and send the cleaned traffic to the customer's network OR use two detection systems, one placed in house or on the data center premise at network perimeter level and the second mitigation system based at the Security Operations Center (SOC) at the Cloud Data center level. These defenses complement each other in providing a quick and early detection for the attack types at the same time ensuring minimum disruption to network and business operations.

- The defense system at Customer Premise preforms traffic analysis, attack detection and signaling by constantly monitoring network traffic and the traffic pattern in order to establish a normal behavior baseline threshold much like an IDS. Then the system is able to detect anomalies and DDoS attacks at initial stage and instantly alert the Data Center Security Operation Center for mitigation.

- When the WAN circuit networks are under a volumetric DDoS attack, customer traffic is routed to the scrubbing data center for blocking and mitigating the traffic. Once the initial filtering is performed, the scrubbed traffic is rerouted to the subscriber's Cloud provider. The Scrubbing center teams collected and stored the attack data for enabling real-time monitoring and historical reporting and analysis.

- There are however issues of compliance and regulations, the need to install detection systems as either a hardware device or a thick client for each customer and data privacy issues for traffic flowing to a third party scrubbing center.

CHAPTER SUMMARY

Traditional IT defense system like On-premise Infrastructure setup, ISP Data center services or third party Scrubbing solutions can hardly be expected to take on the wide range of the new age dynamic DDoS threat vector attacks. DDoS attacks are large enough to overwhelm a service provider's WAN circuit and impact the ability to block or absorb attacks. DDoS attacks are not only disrupting services, but also distracting severity resources while other types of attacks are attempted like Ransomware and issues due to security vulnerabilities in devices.

As the volume and percentage of cloud service consumers increases, more and more home users and corporate employees use personal computers and mobile smartphones for work. This has led to the rise Ransomware and malware infections impacting innocent users. The subsequent chapter dwells upon Ransomware mitigation and presents the malware detection system impacting end user systems globally.