Solutions for DDoS Attacks on Cloud

Akashdeep Bhardwaj
Computer Science
UPES Dehradun
Noida, India
Bhrdwh@yahoo.com

Dr. GVB Subrahmanyam
Cloud Services
Tech Manhidra
Hyderabad, India
Subrahmanyam.gvb@Techmahindra.com

Dr. Vinay Avasthi
Computer Science
UPES
Dehradun, India
Vavasthi@Ddn.uppes.ac.in

Dr. Hanumat G Sastry
Computer Science
UPES
Dehradun, India
Hsastry@Ddn.Upes.ac.in

***Abstract*–The internet has become the key driver for virtually every organization's growth, brand awareness and operational efficiency. Unfortunately cyber terrorists and organized criminals know this fact too. Using a Distributed Denial of Service attack they can deny corporates and end users the access to internet, make web site going slow, and deny access to corporate network and data, unable to service legitimate users. It is not just these that are vulnerable, DDoS attacks are diversions.**

***Keywords:* DoS; DDoS; Cloud Security; Cloud Computing; Scrubbing; CSP**

I. INTRODUCTION TO DENIAL OF SERVICE

Denial of Service attacks are a cyberattack methods to deny legitimate users the access to online web applications (Email, Chat, Ecommerce, and Banking), SaaS, PaaS or IaaS Cloud services and computing resources like network resources or even VoIP infrastructure with a single attack address.

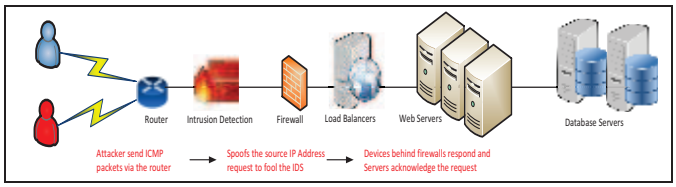

Fig 1. Denial of Service Attack Sequence

Distributed Denial of Service attacks or DDoS attacks simply amplify the effects of a DoS attack by using thousands of machines to launch their assaults, disrupt operations at a large scale by bombarding the target web applications and network devices with information requests that overwhelm the server.

The attacker exploits vulnerable systems across geographies, compromising them by infecting them with a Trojan virus. This is a small application that enables remote access for command and control capabilities of the user systems without their knowledge to attack the intended target servers in an attempt to make one or more services like Cloud services or hosted web applications unavailable to the intended users by send a flood of network packets, data or transaction requests over the network from multiple systems at the same time. These are called Zombies or Bots. These infected systems or bots in turn further compromise others, with the compromised systems working as a group called BotNets.

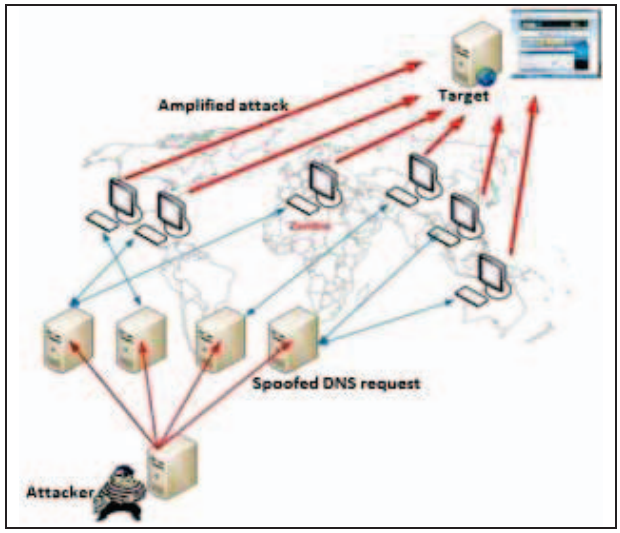

Fig 2. Distributed Denial of Attack Sequence

The problems faced by the users range from:

- Resource exhaustion like over utilizing and consuming the WAN pipes, or server CPU time
- Exploitation for user accounts lockout by repeatedly attempting with invalid credentials
- Process disruption by crashing a web application process by attacking vulnerability in the code
- Pushing a malware that affects processors, opens sockets to triggers errors in computer micro codes
- Corrupting data by altering user types to an invalid type, making it incorrect to input data

978-1-4673-8203-8/16/$31.00 ©2016 IEEE

II. Recent report and Trends

A. As per Akamai and Verizon:

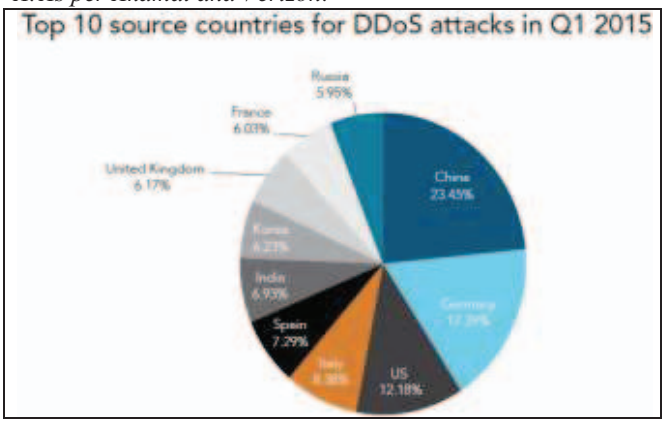

Fig. 3 Top 10 DDoS Attack source locations

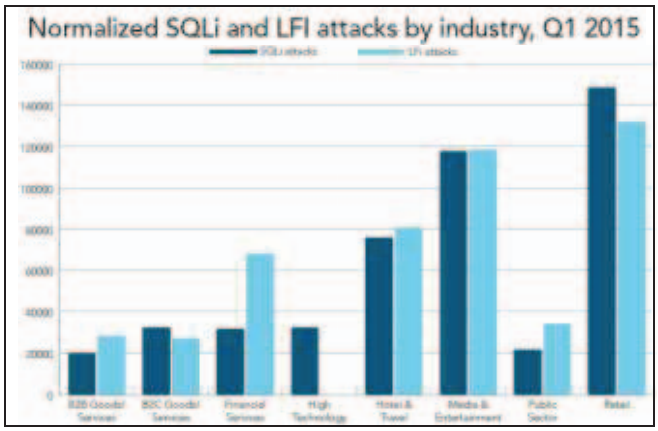

Fig. 4 Top 10 DDoS Attack Targets

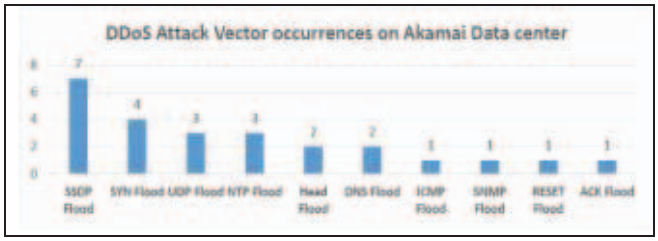

Fig. 5 DDoS Attack Vectors

Infrastructure based attacks had the major share of DDoS attacks as 90% in Q1 2015 as compared to application attacks being about 10%. Some new attack technologies were also tracked that include:

- Joomla and SaaS based applications being targeted by DDoS agents
- Heap-based buffer overflow vulnerability on Linux servers
- Use of new Microsoft SQL Reflection technique by attackers
- Data breach using logon attacks

As per Verisign Q1 2015 for 12 month period reports:

DATA SOURCE	ATTACK DETAILS FOR A ONE-YEAR PERIOD	COMPANIES/INDIVIDUALS SURVEYED
Verisign	63 percent of respondents experienced at least one attack within the preceding year; 11 percent experienced 6 or more attacks; 46 percent said their site was down for 1 or more hours; 25 percent said their site was down for 12+ hours	221 IT executives and decision-makers in the United States; large and medium-sized companies spanning multiple industries, including finance and banking, healthcare, retail, manufacturing and others
Forrester Research	70 percent of respondents reported at least one attack within the preceding year; average attack duration was 2 – 6 hours	400 companies with significant online operations, including online financial services, media, news, political sites, gaming, entertainment, web hosting and e-commerce
Arbor Networks	94 percent of respondents experienced an attack; 47 percent of respondents experienced 1 – 10 attacks per month (i.e., 12 – 120 in preceding year); 47 percent experienced 10 – 500 attacks per month (i.e., 120 – 6,000)	111 Internet service providers (ISPs) and Internet data centers (IDCs) providing access to DNS, wireless, managed security, satellite, hosting, content, web portal, email and other services

DDoS Attack Type Distribution (Q1 2015 – Akamai Report)

In Q1 2015 Simple service discovery protocol or SSDP attacks has become the top infrastructure attack vector, it uses internet connected home systems as attack reflectors by using UPnP (Universal Plug and Play protocol) and bypassed the previous year's SYN Floods. The below charts display the frequency of attack vectors observed in Q1 2015 at the Infrastructure and Application Layers.

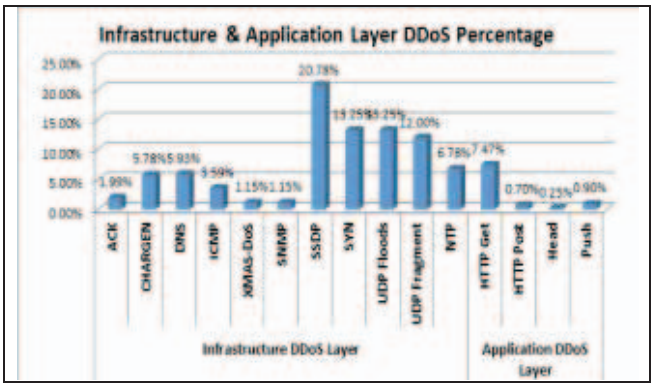

Fig 6. Infrastructure and Application Layer DDoS %

B. Types of DDoS attacks

Depending on the area of the Infrastructure on which the attack is focused, DDoS attacks fall into the following three broad categories:

- Network or Volumetric DDoS Attacks

These clog the WAN circuits connecting the IP bandwidth networks by sending a flood of data packets on the transport layer (TCP or UDP) and network at OSI Layers at level 3 and 4, to have excessive requests overwhelming the connection capacity until the systems are unavailable or just overwhelm the resources and deny the ability to respond to legitimate traffic. The common of these attacks are SYN and DNS floods.

- Application DDoS Attacks

These attacks mimic legitimate user traffic so as to evade an organization's common security measures and try to create bottlenecks in an application or web servers with the goal of

establishing a connection and exhausting it. These sophisticated threats are harder to detect because not many machines are required to attack, generating a low traffic rate that appears to be legitimate.

These attacks overload web servers and databases upon which a Cloud Application service is running and simply flood the Web application with legitimate requests in an attempt to overwhelm server processing power or exploit business logic flaws. The application crashes and takes the site offline. They do not require high volumes, for even a rate of 50 – 100 requests/second is enough to cripple most mid-sized websites.

- TCP State-Exhaustion Attacks

These attacks attempt to consume the connection state tables and actual server resources like CPU or memory or those of intermediate communication equipment which are present in many infrastructure components such as load-balancers, firewalls and the application servers themselves. Devices capable of maintaining state on millions of connections can be taken down by these attacks. These are based on TCP and tend to attacks on the server socket clogs the website, or online service, measured in packets per second.

III. Proposed Solutions to Mitigate DDoS Attacks

With Distributed Denial of Service (DDoS) attacks on Cloud Services becoming the main threat, have having increased multifold in their complexity, flooding volumetric traffic and sophistication worldwide, corporate enterprises, banking, financial and hosting companies have come to realize 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 solutions 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 that we have proposed here. Here are some traditional solutions in use to mitigate DDoS:

A. On-premise based DDoS solution

On premise infrastructure [1] as a private cloud with limited ISP leased bandwidth, basic security devices as firewalls and IDS. 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 in house defense system's inability to protect against volumetric floods – when attacks flood and saturate the ISP WAN circuits and the enterprise defense network themselves, it becomes it a challenge to stop high-volumetric attacks on the networks.
- A second issue is the constant need for an ongoing investment on IT infra, 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 group cannot and invest resources for On-premise infrastructure as a private cloud with limited ISP leased bandwidth, basic security devices as firewalls and IDS. 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 in house defense system's inability to protect against volumetric floods – when attacks flood and saturate the ISP WAN circuits and the enterprise defense network themselves, it becomes it a challenge to stop high-volumetric attacks on the networks.
    - A second issue is the constant need for an ongoing investment on IT infra, 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 group cannot and invest resources needed.

B. ISP DDoS solutions

While ISPs do tend to offer DDOS mitigation as an additional service [2], 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 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 as well.

C. Scrubbing Defense DDoS mitigation

Use of scrubbing defense [3] architecture is performed in two ways for DDoS protection – either 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, 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.

D. Multi-Tiered Network Architecture DDoS mitigation

For enterprises working with critical financial domains or with government organizations, use of three layered network architecture is a much better option. In this model the traffic flows as shown below.

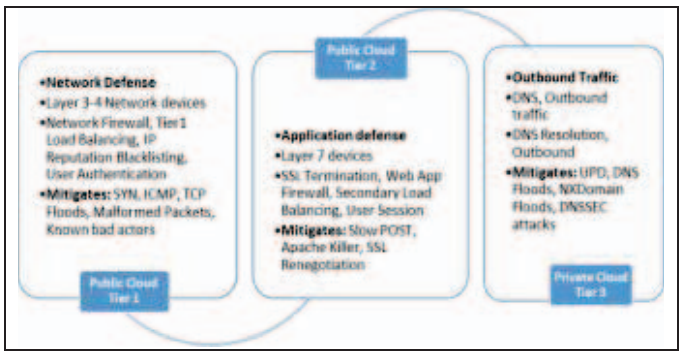

Fig 7. Three *Tiered Network Architecture Design Traffic Flow*

This involves use of Hybrid Cloud model by having two Public clouds which act as defense layers and one Private cloud which hosts the SaaS application and critical database.

- The first two layers are DDoS protection defenses with only legitimate traffic allowed to access a third tier hosting the actual Cloud based Software application and its components like Servers, OS, Virtual Machines, Web portal apps and Database. Data Traffic flow and protection can be visualized as follows.

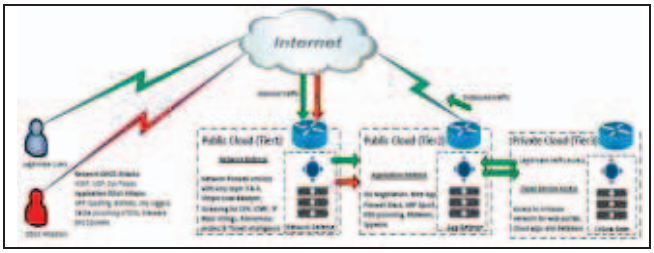

Figure8: Multi-tiered Cloud Data center

The first layer performs network defense, it needs to be setup for only inbound traffic, and can block and mitigating 80 to 90% DDoS attacks at this level. The user traffic passing through the first tier has only level 3 and 4 devices, user data packets are checked for the network attack so SYN Floods and ICMP floods get mitigated here.

The network firewall services and simple load balancing with DNS Services are performed along with IP Blacklisting Reputation check to control the inbound traffic at source data packet level.

The traffic now flows over to the second tier, where application attack checks are performed to mitigate ARP Spoofing, BotNets, Key loggers, Cache poisoning of DNS, Malware and Spyware.

With both tiers being Public Clouds, scalability and provisioning is not an issue, so this caters to volumetric network attacks and application level attacks. The traffic is now has only authenticated, legitimate Cloud service users. This is allowed access to the Web applications and Database of the SaaS Cloud from the third-tier which is a Private data center allowing access to critical data.

Once processed, the traffic is sent back from Tier 3 to the Tier2 data center and then back to the user via the internet.

IV. Conclusion

As the Cloud Computing technology adopts and advances towards embracing Cloud services, DDoS attacks have only increased in the past few years and show no signs of abating in volume, complexity or magnitude. The traditional IT defense systems on premise DDoS solutions or taken from ISPs can hardly be expected to take on the wide range of new types of dynamic attacks.

DDOS attacks are becoming large enough to overwhelm Cloud provider's ability to absorb Server based attacks harness data center computational and networking resources to

stage DDOS attacks of unprecedented volumes. Due to the increased attack volume, collateral damage is becoming a major cause of concern – packet loss, delays, high latency for internet traffic of those whose network traffic simply happens to traverse the WAN saturated by a DDOS attack. DDOS attacks are not only being used to disrupt services, but also to distract security resources while other types of attacks are attempted like fraudulent transactions. Adaptive DDOS attacks are prevalent – attackers attack traffic on the fly to avoid identification and confuse mitigation plans. Reflective and Amplification attacks are most common – leveraging misconfigured DNS, NTP and other network resources by spoofing source IP addresses

The bitter reality is that for cloud computing to be useful, it has to be exposed on the unsecure WANs and public internet. With Cloud services presence being advertised and the interfaces defined unauthorized attacks would always look to target the services.

REFERENCES

[1] Sugam Sharma, U S Tim, Shashi Gadia, and Johnny Wong, "Proliferating Cloud Density through Big Data Ecosystem, Novel XCLOUDX Classification and Emergence of as-a-Service Era", 2015

[2] Sugam Sharma, "Evolution of as-a-Service Era in Cloud. Cornell University Library, 2015

[3] Sugam Sharma, U S Tim, Shashi Gadia, and Johnny Wong, "Growing Cloud Density & as-a-Service Modality and OTH-Cloud Classification in IOT Era", 2015.