A Novel Mechanism to Defend DDoS Attacks Caused by Spam

Abstract Corporate mail services are designed to perform better than public mail services. While corporate mail services are convenient and provide fast mail delivery, ability to transfer large file, provide high level spam and virus protection, and advertisement free environment but they are also frequently targeted by hackers and spammers and thus making this service challenging. These days the DDoS attack through spam is a persistent threat to mail services of various organizations. Spam penetrates through all filters to establish DDoS attacks, which causes serious problems to users and the data. Because spam imposes such significant challenges, should all corporate mail services be considered hostile to the organization? Not necessarily. A well organized corporate mail service protects the system from DDoS attacks. In this paper we propose a novel approach to defend DDoS attack caused by spam mails. This approach is a combination of fine tuning of source filters, content filters, strictly implementing mail policies, educating user, network monitoring and logical solutions to the ongoing attack. We have conducted several experiments in corporate mail services; our analysis shows that this approach is highly efficient to prevent DDoS attack caused by spam. The novel defense mechanism reduced 60% of the incoming spam traffic and repelled many DDoS attacks caused by spam.

Keyword: Spam, DDoS Attack, DNSBL,SURBL,rDNS

1. Introduction

Email is a source of communication for millions of people world wide [8]. But spam abruptly disturbs the email users by eating their resources, time and money. In the Internet community spam has always been considered as bulk and unsolicited. Spam mails accounts for 80% of the entire mail traffic. Many researchers have proposed different solutions to stop spam. But the effort has become a drop of water in the ocean. No matter how hard, spammers always find new ways to deliver spam mail to the user's inbox. Of late, spammers target mail servers to disturb the activities of organizations which results in economic and reputation loss. The DDoS attack is a common mode of attack to cripple the particular server. The spammers take DDoS attack in their arms to disturb the mail servers. In this paper we examine the DDoS attacks through spam mails. We propose a multi layer approach to defend the DDoS attack caused by spam mails. We have implemented this methodology in our mail system and monitored the results. The result shows that our approach is very effective to defend DDoS attack caused by spam.

E-mail life cycle : The composed mail in the source machine will be handover to the Message Transfer Agent (MTA). The MTA will find the destination machine with the help of DNS server and relay the mail to the destination systems MTA [12]. The MTA at the destination machine delivers the mail to the destination user's mail box. The machines between source and destination will act as intermediate machines for the data transfer called relay. MTA relay mail between each other uses the Simple Mail Transfer Protocol.

Corporate mail services usually faster and sophisticated than free mail services. The corporate mail service deliver mails quickly and provides a facility to attach large size files and unlimited storage facilities. To deliver mails faster, the server generally skip most of the time consuming spam protection tests. To attach the big size files it has to bypass several content filter settings. This makes the corporate mail servers vulnerable to spam mail which ultimately causes DDoS attacks. We propose a multi layer approach to defend the DDoS attack caused by spam mails. We implemented this methodology in our mail system and monitored the results. The result shows that our approach is very effective to defend DDoS attack caused by spam.

The rest of the paper is organized as follows. Section 2 discusses related work. Section 3 explains the mechanism of DDoS attack through spam. In section 4, we describe our methodology to defend the attack. Section 5 provides data Collection and experimental results. We conclude in section 6.

2. Related work

In [1] L.H. Gomez et al, presented an extensive study on characteristics of spam traffic in terms of email arrival process, size distribution, the distributions of popularity and temporal locality of email recipients etc., compared with legitimate mail traffic. Their study reveals major differences between spam and non spam mails. In [2] Anirudh R. et al, examines the use of DNS black lists. They have examined seven popular DNSBLs and found that 80% of the spam sources are listed in some DNSBL. A comprehensive study of clustering behavior of spammers and group based anti spam strategies presented by Fulu Li, Mo-han Hsieh [4]. Their study exposed that the spammers has demonstrated clustering structures. They have proposed a group based anti spam frame work to block organized spammers. In [5] Anirudh R. et al, presented a network level behavior of spammers. They have analyzed spammers IP address ranges, modes and characteristics of botnet. Their study reveals that blacklists were remarkably ineffective at detecting spamming relays. Their study states that to trace senders the internet routing structure should be secured. Carl Eklund [8] presented a comprehensive study of spam and spammers technology. His study reveals that few work

email accounts suffer from spam than private email. To the best of our knowledge our study is the first paper, comprehensively studying the DDoS attacks by spam.

3. Mechanism of DDoS attacks through spam

Distributed Denial of Service (DDoS) attack is a large scale, coordinated attack on the availability of services at a victim system or network resource [3]. DDOS attack through spam mail is one of the new versions of common DDoS attack. In this type, the attacker penetrates the network by a small program attached to the spam mail. After the execution of the attached file, the mail server resources will be eaten up by mass mails from other machines in the domain resulting in the denial of services. The working scenario of this attack is shown in fig.1. The attackers take maximum effort to pass through the spam filters and deliver the spam mail to the user's inbox. Here the hackers do enough to make the mail recipient believe that the spam mail is from a legitimate user as shown in fig.2. Social Engineering techniques are used to convince users to open spam mails or attachments [25]. The attackers use fake email ids from the victim's domain to penetrate through the network. The spam mail is sent in the name of Network administrator / well wisher of the victim or boss of the organization. Note that the spam mail does not have the signature of these senders.

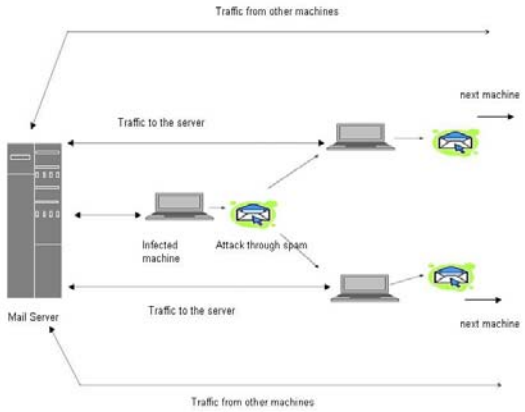

Fig.1. Attack scenario

The spam contains small size of .exe file as an attachment (for example update.exe). The attackers used double file extension to confuse the filter (Update_KB2546_*86.BAK.exe (140k)) and user. The attachment size ranges from 35KB to 180 KB. The spam mail asks the recipient to execute the .exe file to update anti virus software. Upon execution of the attachment, it will drop new files in the windows folder and change the registry file, linked to the attacker's website to download big programs to harm the network further. The infected machine collect email addresses through windows address book and automatically send mails to others in the same domain. Even if the users don't use mail service programs like Outlook express and others, it will send mails by using its own SMTP. Mostly this kind of spam mail attracts group mail ids, and will send mails to large groups. By sending mails to the group, it will spread the attack vigorously. If users forward this mail to others it will worsen the situation. Ultimately the server will receive enormous request from others beyond its processing capacity. In this way the attack will spread and results in DDoS attack. After the first mail, every minute it will send same kind of mail with different subject name and different contents to the group email ids. Very soon it will eat up the server resources and end up in distributed denial of service attack. The names of the worms used in these kind of DDoS attacks are WORM_start.Bt, WORM_STRAT.BG,WORM_STRAT.BR,TROJ_PDROPPER.Q. Upon execution, these worms drop files namely serv.exe, serv.dll, serv.s, serv.wax, E1.dll, rasaw32t.dll etc.

Subject: Mail server report.

Our firewall determined the e-mails containing worm copies are being sent from your computer. Nowadays it happens from many computers, because this is a new virus type (Network Worms). Using the new bug in the Windows, these viruses infect the computer unnoticeably. After the penetrating into the computer the virus harvests all the e-mail addresses and sends the copies of itself to these e-mail addresses.

Please install updates for worm elimination and your computer restoring.

Best regards,

Customers support service

Attachment : Update_KB2546_*86.exe (140k)

Fig.2. Content of spam

DDoS malware cause direct and indirect damage by flooding specific targets [14]. Mass mailers and network worms cause indirect damage when they clog mail servers and network bandwidth. In Network, It will consume the network bandwidth and resources, causing slow mail delivery further resulting Denial of service. The server will be down due to enormous request from clients and bulk mail processing. It might also crash due to over load. For Individual user, by receiving unlimited number of spam mails, the user will be frustrated and they will not be able find legitimate mails. User can't use Internet explorer and other applications due the files dropped in system folder. The system becomes unusable and system data or files become unrecoverable. It will automatically load many programs in system startup and therefore it takes long time to boot and shutdown the system. It will change the registry settings of the individual machines as well as corrupt the data.

In E-Mail Bomb Attacks, thousands of e-mails are sent to a single target to fill the storage space or bandwidth of the target [24]. If the mailbox is filled with the spam mails, the user cannot receive legitimate mails. This situation is similar to the results of DoS attacks. Email spamming is another version of Bombing. The spammers can send thousands of mails to the users in a single domain causing the mail server to overload. The software tools are available in Internet to send 350 spam mails per minute on 1mbit cable [11]. Ultimately it will result the Denial of service attacks on the server. Hundreds of spam mail tools are freely available on Internet for example Phasma Email Spoofer, Bulk Mailer, Aneima 2.0, Avalanche2,3.5, Euthanasia etc.,

4. Proposed Defense Mechanism

We proposed a multi layer approach to defend the DDoS attack caused by spam mails. We implemented this approach in our mail system and monitored the results.

The result shows that our approach is very effective. The approach has six layers as shown in fig.3. This approach is a combination of fine tuning of source filters, content filters, network monitoring policy, general email policies, educating the user and timely logical solutions of the network administrator. Fine tuning of source filters reject the incoming connections before the spam mail is delivered. The content filters analyses the contents of the mails and blocks the incoming unwanted mails. Network monitoring approach provides general solution to identify the attacks prior to the attack and also during the attack. Business houses should educate the user about possible attack scenarios and ways to handle it. The logical solutions of the network administrator play an important role during the attack period and even post attack period. The combination of these layers provides best methodology to stop the DDoS attacks established though spam mails.

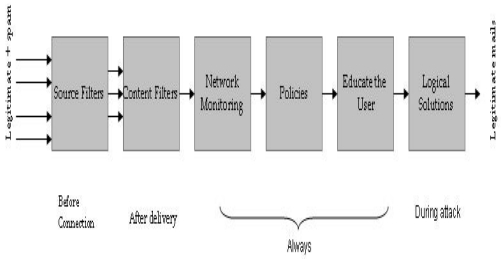

Fig. 3. Defense Mechanism

4.1 Source Filters

There is a prediction that the spam will be 80% of the email traffic in 2007[1]. Lot of source filters are available in real time. But by simply enabling all filters will not help to prevent attacks. It will slow down the mail delivery process. So the fine tuning of filters is an important way to handle attacks. The fig.4 shows the structure of the filters.

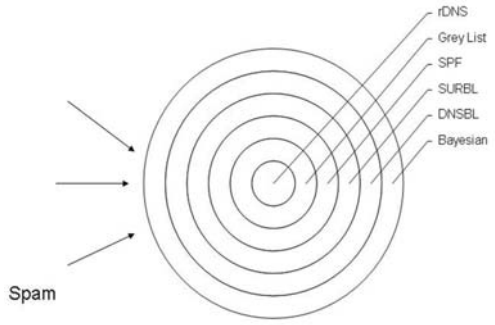

Fig. 4. Combination of Source Filters

Bayesian Filter : Bayesian filtering is one of the effective filtering technologies used by most antispam software developers [9]. This filter works based on the mathematical theorem of Bayes a British mathematician. Anti spam developers have developed various algorithms by modifying the Bayes theorem to effectively filter the spam.

In Bayes methodology, the system develops two tables from the contents of incoming spam mail & out bound legitimate mails. The tables are referred as a dictionary. Each word from an incoming new mail will be compared to the spam mail table and legitimate mail table or dictionary. For incoming mail words, the probability value is calculated based on the number of occurrences of particular word in spam mail table and legitimate mail table.

For example the word “Viagra” occurs 400 times in 3000 spam mails and in 5 out of 300 legitimate mails the probability would be .889 [400/3000]/ [5/300+400/3000]. It will perform the same operation for all words in the incoming mails. The mail is classified as spam, if the calculated probability is higher than a given threshold mostly above 0.5. The normal threshold value ranges from .7 and above for a corporate mail server. Based on the threat level the administrator can change the threshold value. After the classification of the mail as a spam, the contents of the spam will be added to the dictionary. It will be useful for the future calculation. In this way the system will learn the latest technologies used by the spammers. The administrator can enable or disable the learning from the spam and outbound mails. Most of the filters offer an administrator to select the number of words for the dictionary. We recommend 50000 words are recommended for small and medium sized mail server. If you increase the dictionary size, the lookup time or processing time will increase causing the delay in the mail delivery. The system will take two weeks to build a spam word table but some of the filters use static tables. Bayesian filter is the most important and successful antispam method [9]**.**Though powerful, the spammers have learned how to pass this filter to deliver spam into inbox even it is powered with learning. Enhancement techniques may be useful [12] but an ever increasing the quality of filter is impossible since the dictionary size and the content of the mail is limited. “Mail, server, report, firewall, virus, windows, customer, support” are some of the common tokens listed in legitimate mail table and also used by the attacker in the given sample mail [fig.2.] The server will send a regular report titled “server report” to the network administrator. So the probability of being spam for this mail is very less which results safe delivery to the user’s inbox. After the attack the system will add these tokens to the spam tokens table. The legitimate mail word table is a standard one and new words can’t be added through learning. The hackers can get data and use it to bypass the filters. Bayesian filtering is effective but it can not filter 100% of the spam. With the combination of various filters Bayesian Filter will work more effectively and overall the performance of spam filtering can be increased.

DNSBL : Even though the spam generation is not accepted widely as a legal actively, 80% of the spam mail is generated by particular users. If we have the list of these spam generators IP addresses, we can effectively block the spam messages. DNSBL is based on the above said concept. DNS black hole list or black list is a well defined source filtering technology it works before delivering the mail to the user’s inbox. The DNSBL publishes the list of IP addresses through DNS of massive spam generators. DNSBL offers various list of IP addresses based on open relay, spam or virus source. The most widely used DNSBL are spamhaus, spamcop,sorbs, abuseat,dsbl, rfc-ignorant etc., these DNSBLs list out thousands of IP addresses of spam generators. By blocking this well known IP addresses we can effectively block the incoming spam traffic. There

might be a overlapping of IP addresses in various Black lists [5]. Due to this the legitimate mail delivery will be delayed if there is overlapping of IP addresses and if there are too many BL are included in the DNSBL. The IP address of the black listed IP addresses will change frequently based on their spam generating behaviors. Some DNSBLs will check the particular IP address regularly; if they stop the spamming activity, it will remove the particular IP address and add the new IP addresses of spammers [2].

If we enable "immediately reject the connections" from blacklisted server option, the connection will not be established to the particular spammer. Mail servers usually provide option to include more lists or delete the DNSBLs from the list. But the remaining 20% of the spam mail generators are not listed by any DNSBL, we had to depend on other filters or methodologies to stop spam. Since the spammers change their IP addresses frequently, there is no single blacklist with all the complete spam generating IP addresses. Moreover these list providers are frequent target to hackers. The spammers used Mimail.E worm to perform Dos attack on spamhaus site. In 2003, Spamhaus servers came under distributed Denial of Service (DDoS) attacks by thousands of virus-infected computers throughout the Internet [20]. In 2006 also the spamhaus servers were out of service due to DDoS attacks [25]. It is clear that the angry spammers try to stop the services of DNSBL. These attacks clearly show the use of more than one DNSBL in the List. Even if one DNS black list is out of service the mail server can manage with other lists. In recent days the DNSBL lookups have increased tremendously when compared to 5 years before [3]. Nearly 80% of the spam generated by relays that appear in one at least one of eight major blacklists [4]. Fine tuning of multiple black lists is more effective than simply using all lists. The DNSBLs is not effective if the spam is being sent from large set of IP addresses [2].

SURBL : SURBL searches for URLs in the incoming mails. SURBL is a collection of spam supported websites, domains, web servers. If there is any URL or IP address in the message, the system will contact the SURBL list to check whether the URL is listed. If the URL is listed in SURBLs, it blocks the messages. The available SURBL lists are sc.surbl.org, ws.surbl.org, ob.surbl.org, ab.surbl.org. multi.surbl.org is a combination of all the lists. If the system uses other SURBLs with multi.surbl.org, it will take long time to process the mail. If we use only multi.surbl.org for SURBL check, and if the service is not available, no checks will be performed. We recommend using other four surbls rather than multi.surbl.org. The administrator can edit the list whenever a high rate of false positive is present [17].

In the attack mentioned in section 2, the worm downloaded malicious code from the following websites.

http://www2.{BLOCKED}tinmdesachlion.com
http://www3.{BLOCKED}tinmdesachlion.com
http://www4.{BLOCKED}tinmdesachlion.com
http://www6.{BLOCKED}tinmdesachlion.com

If SURBL was enabled, there were less possibility of the attack. This kind of URL based filter is very effective against the DDoS attack since these references are faked websites. Some attackers include multi URLs to confuse the filters. For multi domain messages, it is hard to determine the real spam domain among all the domains [10]. The combination of checking SURBL database with other filters is a best way to defend the DDoS attacks.

Sender Policy Framework : Sender Policy Framework reject message, if SPF test is fail or soft fail [15]. Sender address forgery is a big threat to the users as well as the entire network. In the attack mentioned in the section 2, all the users received mails from the unknown person within their organization. The attacker's mail id is fake with the domain name extension. That is why most of the users obey the instruction and execute the file attachment leading to DDoS attack. We can stop this kind of forgery by SPF (Sender Policy Framework).The current version of SPF is called SPFv1 or SPF Classic [15]. The Sender Policy Framework allows you to check whether a particular email sender is forged or not. Most of today's spammers use forged email addresses to hide their identity. SPF requires that the organization of the sender has published its mail server in an SPF record. If you receive a mail from a user, you can check of that mail is coming from a particular organization by the sender's IP address. The SPF record will inform the receiver whether the user is allowed to use their network or not [15]. If the organization recognizes a particular machine, it passes the test. Otherwise it is an attacker or a spammer. There are two types of fails namely fail and soft fail.

Grey Listing : Grey listing is a simple technique to fight against spam [18]. It will reject all incoming mails from unfamiliar IP addresses with an error code. The mail server records the combination of sender, recipient id and IP address. If the same sender is trying to send the mail after 10 seconds to 12 hours, the server will check for the combination in its record, if it matches, it will allow the sender to deliver the message. This is based on assumption that the spammers will not try again but legitimate users. Spammers learned this technology to bypass filters. But results show that there is substantial reduction of spam after the implementation of grey listing. The old version of Grey list used to accept the second mail after 4 hours [19]. But the legitimate user faces delay in mail delivery.

Reverse DNS : The incoming system should have rDNS set. The sending system should give a domain name and IP address to prove that is from the legitimate user. Most spam don't have reverse DNS [12]. Rejecting all incoming mails without rDNS is an effective way to filter spam. The two options supported by most mail services are "Reject message if sending server IP does not have a reverse DNS entry", "Reject message if the reverse DNS entry does not match Helo host". SPF and rDNS are good to filterto some extends.

4.2 Content Filters

Once cleared from the SMTP server, the sender is allowed to deliver the message headers and body of the mail [12]. By carefully checking every word of the header and contents we can still block spam. Most spam headers try to confuse the filters. Spammers use

recognizable words as a subject and clear from address. If the incoming mail has particular content or subject, the content filter will stop the mail delivery. Most spam that causes DDoS attack have subjects like test, server report, status, helo etc; In this case the attacker carefully selected the words to avoid the content filtering. “Server report” is a word used by servers to send report to the administrator. The content filter blocks the mail which has some specific words like Viagra, ViAgRa, install updates, customer support service etc. Multiple words separated by comma and space are allowed in content filters to search the mail contents.

Most manuals say that the blocking of particular id and IP address is not useful [24]. But by doing so spam mail delivery is highly reduced. Even blocking the entire sender domain is highly advisable to stop further spam delivery or attack. But in this DDoS attack, further attacks were from its own domain mail ids except the first mail. Blocking own mail id is not possible. Another option of content filter is if you know your regular contacts, you can block all other mail senders. We can block mails not send by a particular user. If the administrator doesn’t want to receive mail from other mail ids rather than own domain ids, he can block all incoming and outgoing mails by enabling option “Block incoming message not sent by “. Content filters allow the administrator to block all mails with big size attachments. For example he can block all incoming mails of the attachment size is more than XY KB. In this case the attacker can not deliver attachment with worms which are large in size. This will completely block the DDoS attack. Moreover chances of DDoS attack caused by dumping larger size files will be eliminated at a greater extend. Denial of service will be delayed from the starting time of the attack. The administrator can take other steps to defend the DDoS attack during the delay time.

The content filters can block mails with particular type of file as an attachment [12]. Most of these worms have .exe as extension. If the filters block all the incoming mails with .exe file as attachment the incoming DDoS attackers can be stopped. But these days the spammers have learnt this and started to send attachments with double extension like update.doc.exe, update.txt.exe etc. This will confuse the filter and will be delivered to mailbox. To avoid this, content filter provides the options like *.*.exe. This kind of technique is helpful to defend the DDoS attacks through spam. Before the attack, the content filters can not identify the contents, headers, subject, and the attachment size and file extension of the incoming mails. After the first mails the administrator can identify these item and block by using content filters. The experience of the administrators can play a wide role in this filter. While all the filters are effective to some extent, a combination of these filters will effectively stop the DDoS attacks through spam mails. Even if it passes through one filter, it will be blocked by another one. After the initial attack the combination of content filters play an important role to defend the DDoS attacks caused by spammer.

4.3. Policies

Mail is the primary source of communication between all employees in an organization. Therefore it is appropriate that an email-etiquette be established to distinguish between what is Push vs. Pull information. As any organization of any size, it needs an agreed upon system of sending, sorting and utilizing files in their mail server. The type and number of emails / files sent via mail has increased exponentially over the past few years. If the server reaches its maximum capacity level it might cause significant delay in email ultimately results DoS. Setting up policy will help the organization to have a reliable mail system.

Mail Policy: Departing staff will have their organizations account automatically closed after a month following their departure. This will stop easy attacks from insider or ex employee. Further it will reduce the server load. Bulk emailing (ie, allstaff@ABC.com, allnonostaff@ABC.com etc.) should be accessible only by the Administration. For example if allstaff is a group id with has 250 users, one mail will be delivered to 250 inboxes. If the attacker uses this id, it is easy to implement DDoS attack very soon. To stop this all the mail users should not be allowed to use this mailing group ids except if deemed necessary. Since the DDoS attack through spam mail targets only group ids, this will prevent attacks to some extent. If these group mail ids are private i.e open to only insiders to view and only to particular persons to post mail, it will completely eliminate the possibility of the DDoS attack through the spam mails. Email Attachments sizes should be restricted. So bulk mail spamming will be stopped by filters. Attachment files with .exe or double extensions should be blocked.

The users required to use signatures or administrator should set default signatures to all ids in the domain. This will help the users differentiate between spam and legitimate mail. Mostly the attackers’ mail will not contain any signatures. Also the users can be encouraged to use specific words in certain place. For example if the organization is religious organization, force all the users to use particular word to identify the mail is from legitimate user. For example if all the users can use “In His Service” instead of “regards” at the end of the mail. The attackers can not identify such words to make the user to believe the mail is from legitimate user. Most of the DDoS attacks through spam mail take extra effort to make the user to believe the mails are from legitimate user. Since most of the attack mails sent in the name of network administrator or head of the Institute, these unique code words will separate the spam from legitimate mails and the user will not open the mail or execute the attached file. It will help the network to fight against DDoS attacks through spam effectively.

4.4. Educate users

The user’s action during the attack or before the attack plays an important role to defend the DDoS attacks. So the users need to be educated as how to behave generally during an attack. The users have to be educated about spam mails and DDOS attacks. The users should be asked not to open or reply or forward or any kind of mails from unknown users. The user should inform the network administrator, if they have responded to the spam. The users can choose to flag spam so that the server knows to block it. The users should be asked not to use their work email addresses when registering for non-work related activity such downloading music files or online shopping etc. They should also be asked not to run any exe file or any file sent as attachment. Automatically deleting spam every day should be implemented. If not, users should be advised to clean up their spam regularly. After the attack if

spam mail exists with DDoS attack weapon, by mistake it can reappear and result DDoS attack. So the users should clear their old mail and spam regularly.

4.5. Monitoring the Network

To defend the network against DDoS attack through spam requires real time monitoring of the network traffic to obtain timely and important information. Monitoring the performance of the network plays an important role to avert the DDOS attack [14]. Unusual activities can be detected, if the network is monitored 24*7. If the speed of the mail service is slow, we can assume that the server is processing a bulk data. Even the heavy regular network traffic causes congestion; the administrator should regulate data flow by his regular procedures to increase the speed. But during the attack, the net administrators not to be ease the data flow by his regular practices. This indicates that there is something wrong in the network. If the DDoS attack takes place automatically the mail server's speed will go down. Continuously monitoring the network performance is a useful practice to defend the attack. We monitored two mail servers simultaneously with 200 mail users in the domain. In one domain the attacker launched DDoS attack through spam, because of continuous monitoring the net administrator marked the mail as a spam and deleted before it spread to others. The domain escaped from the attack. In another domain for experiment, the spam was not marked and was allowed to the user's inbox. Some of the users responded to the spam by forwarding and executing the mail. Since this attack targeted only group ids, the mail server was out of service with in a day. Maintaining the history of network activities and network problems are useful to handle situation like this. By experiences we can provide logical solution to DDoS attacks through spam.

4.6. Logical solutions

By the network administrator's skills any attack can be handled with minimum impact. After the attack, shutting down the server is not useful. Ways should be identified to change the path of the data dumping. The DDoS attack through spam mail targets only group ids. So the mail service will become out of service quickly. But the net administrator can change all the group ids to new ids. For example allstaff@ABC.com can be changed to all_staff@ABC.com. These group mail ids can be converted to private users and not allowed for public mailing. This prevents the attacker to send further mails. Since the incoming spam has been diverted, all spam can be stopped immediately. But already infected machines can create problems. The infected machines need to be removed from the network. In order to view the impact of the attack, these machines have to be analyzed. After the removal of worms from these machines, they can be allowed to join the network. There will be a logical solution to every attack, no need to be panic.

5. Data Collection and Results

We have conducted several experiments to measure the effectiveness of DNSBL, SURBL and the proposed defense mechanism. The tests were conducted on client computers connected through local area network. The web server provides service to 200 users with 20 group email IDs and 200 individual mail IDs. The speed of the Internet connection is 100 Mpbs for the LAN, with 20 Mbps upload and download speed (Due to security and privacy concerns we are not able to disclose the real domain name). Our dataset consists of spam mails collected at a large spam trap. The trap is a collection of spam mails filtered by source, content filters, and other settings mentioned in this paper.

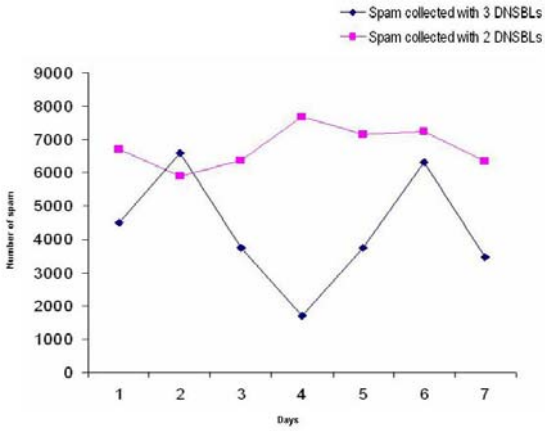

Fig.5. Effectiveness of DNSBL

Several experiments were conducted to measure the effectiveness of DNSBL. Relays.ordb.org, bl.spamcop.net, sbl.spamhaus.org is a good combination to effectively filter spam. For continues seven days we have enabled relays.ordb.org, bl.spamcop.net, sbl.spamhaus.org in the DNS black lists and collected the spam. Later we removed relays.ordb.org from DNSBL list and measured the spam trap. When we removed relays.ordb.org from the list, we observed 40~50% increase of spam traffic as shown in Fig.5. Apart from this each user received 2~3 false negatives per day. The standard deviation of false negatives received by an end user for 7 days is shown in Fig.6.

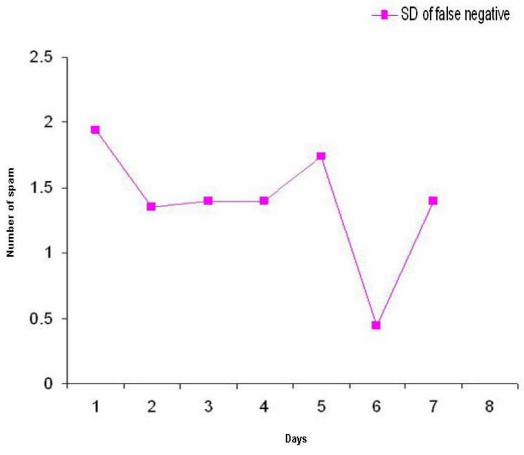

Fig.6. Standard Deviation of false negative

We conducted several experiments to measure the effectiveness of SURBL. The test was conducted in the same network. To test the SURBL, we observed mail delivery for a particular period of time (sessions). Each session is about 3 hour period of time. The experiment result shows that the effectiveness of the SURBL test. Our dataset consists of the spam mails collected at a large spam trap.

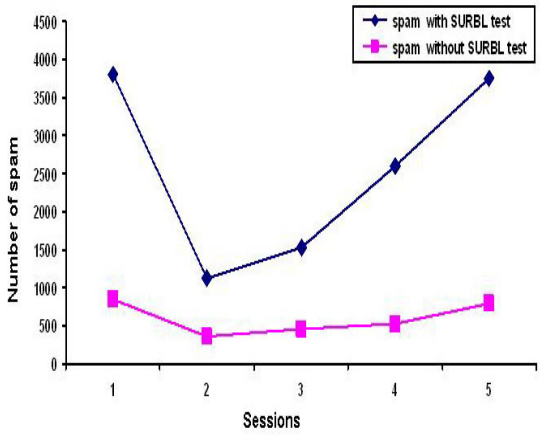

Fig.7. SURBL test-Spam delivery

SURBL test was unchecked for five sessions. The number of spam had increased to the user's inbox when the SURBL test is unchecked; at the same time the number spam has decreased to the spam trap. Most of the users received spam in their inbox during this test. The results are shown in the Fig.7.

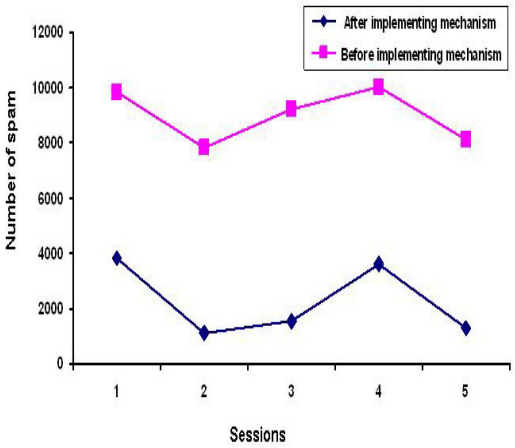

Fig.8. Defense Mechanism effects

Several experiments were conducted to measure the effectiveness of the proposed defense mechanism. We observed the system for six months continuously. Our dataset consists of the spam mails collected at a large spam trap. The graph shows the number of spam received before and after implementing the defense mechanism. We have selected five sessions of data to display. As shown in Fig.8, a session holds good for three hours. The graph shows that after implementing the defense mechanism the incoming spam was reduced by 50 to 60%. Our corporate mail service did not face any DDoS attack for past six months. We have observed that the individual users didn't receive more spam like before implement the defense mechanism.

Before implementing the defense mechanism the mail service used to suffer frequently by DDoS attack. We observed a 100% reduction of DDoS attack caused by spam after implementing the suggested defense mechanism. The spam that causes DDoS attack was diverted to the spam trap. The Fig. 9 shows the number of DDoS attack caused spams which are blocked from reaching the end users, for a period of 6 weeks from January 1 to February 15. The x axis is a week and y axis is the number of spam intended to launch DDoS attacks. Roughly the DDoS attack spam ranges from 180 to 640 with an average rate of 427.

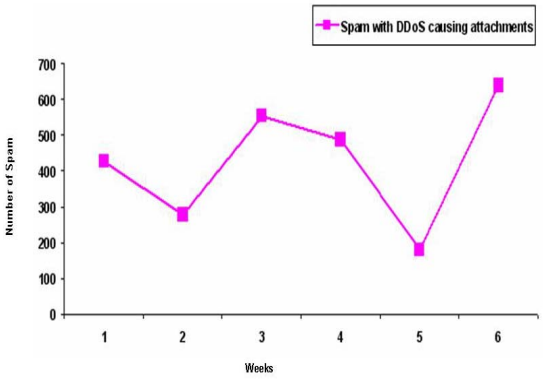

Fig .9. DDoS attack causing spam dataset

6. Conclusion

In this paper we have proposed a multi layer defense mechanism to defend the mail services from DDoS attacks caused by spam. Experimental results show that this system is highly effective and the mail service experienced strong protection against DDoS attacks caused by spam. There is no single step solution to the DDoS attacks established through spam mails. Simply using various filters doesn't stop the possible DDoS attacks caused by spam. But fine tuning of filters mentioned in our mechanism prevents DDoS attacks through spam. The content filter clogs the attack by filtering the spam with unwanted contents and programs. Continuous monitoring of the network averted possible attacks and gave enough time to defend the attacks. Since the users were educated, they responded well to this kind of attacks. The policies prevent the spam mails entering the domain. Last but certainly not the least, the logical solutions to these attacks play an important role to stop these attacks. The experiments show the effectiveness of SURBL to filter spam. The experimental results show that there is 60% of reduction in spam traffic after implementing the defense mechanism. Also we didn't face DDoS attack through spam for the past six months.

References

[1] Luiz Henrique Gomes, Wanger Meira Jr et al : Characterizing a Spam Traffic, ACM IMC-04, pp 356-369,2004.

[2] Anirudh Ramachandran, David Dagon, Nick Feamster: Can DNS-based Blacklists keep up with Bots, CEAS 2006, July 27-28, 2006.

[3] Jae Yeon Jung, Emil sit: An empirical study of spam traffic and the use of DNS Black lists, ACM SIGCOMM Internet measurement conferences, pp 370-75, 2004.

[4] Fulu Li, Mo-han Hsieh: An empirical study of clustering behavior of spammers and Group based Anti-spam strategies, CEAS 2006, pp 21-28, 2006.

[5] Anirudh Ramachandran, Nick Feamster : Understanding the network level behaviour of spammers, SIGCOMM 06, September 2006.

[6] Ben Adida, David Chau, susan Hohenberger, Ronald L rivest: Lightweight Signatures for Email, DIMACS, 2006.

[7] David A Turner, Daniel M Havey: Controlling spam through Lightweight currency, ICCS-04, 2004.

[8] Carl Eklund: Spam -from nuisance to Internet Infestation, Peer to Peer and SPAM in the Internet Raimo Kantola's technical report, 126-134, 2004.

[9] Vladimir Mijatovic: Mechanism for detecting and prevention of email spamming, Peer to Peer and SPAM in the Internet Raimo Kantola's technical report, 135-145, 2004.

[10] Keno Albrecht, Nicolas Burri, Roger Wattenhofer: Spamato-An extendable spam filter system, Keno Albrecht, Nicolas Burri, Roger Wattenhofer, CEAS-05, July 2005.

[11] Jean-Marc Seigneur, Nathan Dimmock, Ciaran Bryce, Christain Damsgaard Jensen: Combating spam with TEA (Trustworthy email addresses) PST 2004, 47-58, 2004.

[12] Technical response to spam, Taughannok networks, Technical report, November 2003.

[13] Ralph F Wilson: SPF helps Legitimate E-mail get through spam filters, Web marketing today premium, Issue 85, November 2004.

[14] Jian Yuan, Kevin Mills: Monitoring the effect of Macroscopic Effect of DDOS flooding attacks, IEEE Transactions on Dependable and Secure Computing, Volume 2, No. 4, pp. 324-335, 2005.

[15] Sender Policy Framework, http://new.openspf.org/

[16] Spamhaus survives DDoS attack http://www.virus.org/news, September 2006.

[17] SURBL http://www.surbl.org/lists.html

[18] Grey Listing-http://greylisting.org/

[19] Greylisting FAQ https://hdc.tamu.edu/

[20] The Spamhous Project. www.spamhaus.org

[21]SpamAssassin
www.spamassassin.apache.org

[22] SpamCop http://spamcop.net

[23] Cloudmark, http://www.cloudmark.com

[24] Email Bombing and Spamming: www.cert.org/tech_tips/email_bombing_spamming.html

[25] Dhinaharan Nagamalai, Cynthia Dhinakaran, Jae-Kwang Lee : Multi Layer Approach to Defend DDoS Attacks Caused by Spam, MUE-07, 97-102, April 2007.

[26] Ben Laurie, Richard Clayton: Proof of work proves not to work, WEIS04, Minneapolis MN, May 13-14, 2004

[27] Guangsen Zhang, Manish Parashar: Cooperative mechanism against DDOS attacks, SAM 2005, pg 86-96, June, 2005