Multi Layer Approach to Defend DDoS Attacks Caused by Spam

Abstract

Corporate mail services are designed to perform better than public mail services. Fast mail delivery, large size file transfer as an attachments, high level spam and virus protection, commercial advertisement free environment are some of the advantages worth to mention. But these mail services are frequent target of hackers and spammers. Distributed Denial of service attacks are becoming more common and sophisticated. The researchers have proposed various solutions to the DDOS attacks. Can we stop these kinds of attacks with available technology? These days the DDoS attack through spam has increased and disturbed the mail services of various organizations. Spam penetrates through all the filters to establish DDoS attacks, which causes serious problems to users and the data. In this paper we propose a multilayer 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; the results show that this approach is highly effective to prevent DDoS attack caused by spam. The defense mechanism reduced 60% of the incoming spam traffic and repelled many DDoS attacks caused by spam

1. Introduction

Email is a source of communication for millions of people world wide [8]. But spam is abruptly disturbing the email users by eating their resource, time & money. In Internet community the spam has always been considered as bulk and unsolicited. Spam mails accounts for 70% of the entire mail traffic [1]. Many researchers have proposed different solutions to stop the 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 the spammers target the 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. This paper is going to study the DDoS attacks through spam mails. We proposed 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 provides background on mechanism of DDOS attack through spam and the effects. In section 3, we describe our mechanism to defend the attack. Section 4 provides data Collection and experimental results. We conclude in section 5.

2. 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 results denial of services. The working scenario of this attack is explained 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 are doing enough to make the mail recipient to believe that the spam mail is from the legitimate user. The attackers use fake email ids from victim domains to penetrate the network. The spam mail had 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.
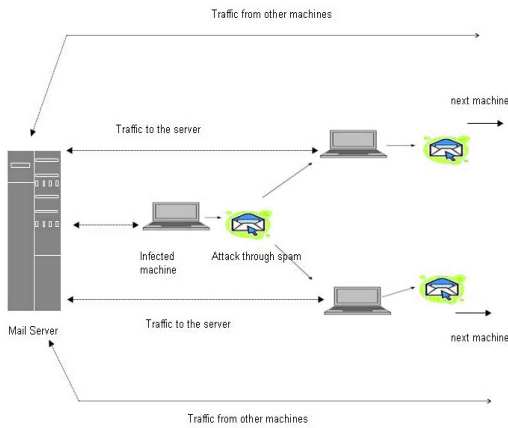

Figure 1. Attack scenario

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 140 to 180 KB. Mostly 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 windows folder and change the registry file, link to the attacker's website to download big programs to harm the network further. The infected machine collected 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 the group mail ids, and will send mails to groups. By sending mails to the group, it will spread the attack vigorously. If any of the 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 it will spread the attack and results in a DDoS attack. After the first mail, for every minute it will send same kind of mail with different subject name & different contents to the group email ids. Rapidly it will eat up 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 dropped files namely serv.exe, serv.dll, serv.s, serv.wax, E1.dll, rasaw32t.dll etc.

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.
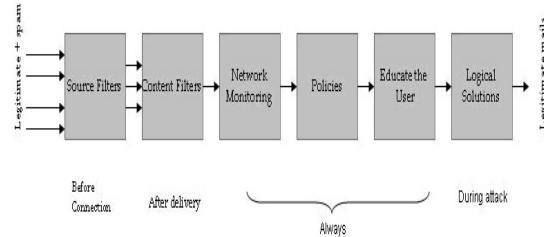
3. Proposed Defense Mechanism

Figure 2. Defense Mechanism Layers

We proposed a multi layer approach to defend the DDoS attack caused by spam mails [Figure 2]. 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.2. This approach is a combination of fine tuning of source filters, content filters, network monitoring policy, general email policies, educating the user & timely logical solutions of a network administrator. Fine tuning of source filters reject the incoming connections before the spam mail delivery. 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 & reacting ways to 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.

3.1. Source Filters

There is a prediction that the spam will be 70% of the email traffic in 2007[1]. There are lot of source filters are available in real time. But by simply enabling all the filters will not help to prevent the attacks. It will slow down the mail delivery process. So the fine tuning of filter is an important to handle the attacks. The figure .3 shows the structure of the filters.

3.1.1. Bayesian Filter. Bayesian filtering is one of the effective filtering technologies used by most of the antispam software developers [9]. This filter works based on the mathematical theorem of Bayes a British mathematician.
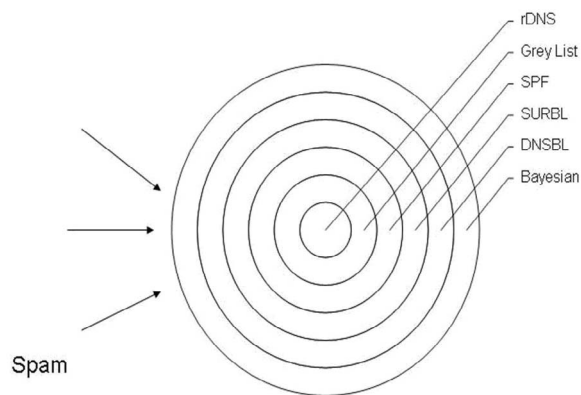

Figure 3. Combination of Source Filters

Anti spam companies 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 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 & legitimate mail table.

3.1.2. 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 concept above said. 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 list publishes the list of IP addresses through DNS of massive spam generators. Lot of DNSBLs offers various list of IP addresses based on open relay, spam or virus source. The most widely used DNSBLs are spamhaus, spamcop,sorbs, abuseat,dsbl, rfc-ignorant etc., these DNSBLs list out thousands of IP addresses of spam generators. 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].

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 are out of service due to DDoS attacks [25]. It is clear that the angry spammers are trying to stop the services of DNSBLs. These attacks clearly show the use more than one DNSBLs 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 are increased tremendously of total DNS lookups compared to 5 years before [1]. 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 when the spam is being sent from larger set of IP addresses [2].

3.1.3. SURBL. SURBL Searches for URLs in 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 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 mentioned DDoS attack through spam [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 was 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 attacker includes 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.

3.1.4. Sender Policy Framework.
Sender Policy Framework reject message if SPF test is fail or soft fail [23]. 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 a fake, it has victims domain name. That is why most of the users obeyed the instruction and executed the file attachment leading to the DDoS attack. We can stop this kind of forgery by SPF (Sender Policy Framework).The current version of SPF — called SPFv1 or SPF Classic [13].

3.1.5. 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 & 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. But spammers learned this technology & how to bypass. 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.

3.1.6. Reverse DNS.
The incoming system should have rDNS ie. The sending system should give domain name and IP address to prove that is from the legitimate user. Most of the spam doesn't have reverse DNS [12]. Rejecting all incoming mails without rDNS is an effective way to filter the spam. "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" are two options supported by most mail services. SPF & rDNS are useful to filter the spam into some extends.

3.2. 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 each and every word of the header and contents still we can block the spam. Most spam headers try to confuse the filters. Spammers will 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 of the spam caused DDOS attack has 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, space are allowed in content filters to search the mail contents. The content filters can block the mails with particular type of files as an attachment [12].

3.3. Policies

Mail is the primary source of communication between all employees at 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 capacity levels that cause significant delay in email ultimately results DOS. The policy helps to avoid the DDoS attack kind of situations.

3.4. Educate the user

The user's action during the attack and before the attack plays an important role to defend the DDoS attacks. So the users need to be educated how to behave generally and during the 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 activities to the mails from unknown users. The user should inform the network administrator, if they responded to the spam in any method. The user 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 in news groups and others. They should also be asked not to run any exe file or any file sent by email. Automatically deleting spam after particular day should be implemented. If not user should be advised to clean up their spam regularly. After the attack if spam mail exists with DDoS attack weapon, by error it can reappear and results DDoS attack. So the users should clear their old mail and spam regularly.

3.5. Monitoring the Network

To defend network against DDoS attack through spam requires real time monitoring of network wide traffic to obtain timely and important information. Monitoring the performance of network plays an important role to avert the DDOS attack [14]. Unusual activities can be detected, if the network is monitored by 24*7. If the speed of the mail service is down, we can assume that the server is processing a bulk data. Even the heavy regular network traffic causes the congestion; the administrator can regulate the data flow by his regular procedures to increase the speed. But during the attack, the net admin can not ease the data flow by his regular practices. It 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.

3.6. Logical solutions

Any attack can be handled with minimum impact by the network administrator's skills. After the attack, shutting down the server is not useful. The ways should be identified to change the path of the data dumping. The DDoS attack through spam mail targeted only group ids. So the mail service will become out of service very soon. But the wise net administrator can change all the group ids to new ids. For example allstaff@ABC.com can be changed in to all_staff@ABC.com. These group mail ids are converted into private users and not for public users. So the attacker is not allowed to send more mails. Since the incoming spam has diverted, all the spam mails stopped immediately. But already infected machines will give trouble to the particular users. 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.

4. Data Collection and Results

We have conducted several experiments to measure the effectiveness of SURBL and the proposed defense mechanism. The test was 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 the 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.

We conducted several experiments to measure the effectiveness of SURBL. To test the SURBL, we observed mail delivery for particular period of time (sessions). Each session is about 3 hours 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.
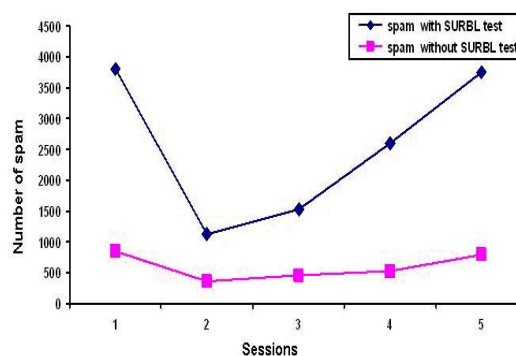

Figure 4. SURBL test-Spam delivery

The number of spam had increased to the user's inbox when the SURBL test is not conducted to check the spam; at the same time the number spam has decreased to the spam trap. SURBL test was unchecked for five sessions. Most of the users received spam in their inbox during this test. The results are shown in the Figure 4.

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 Figure 5, a session holds good for three hours. The graph shows that after implementing the defense mechanism the incoming spam has 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 are not receiving more spam like before implementing the defense mechanism.
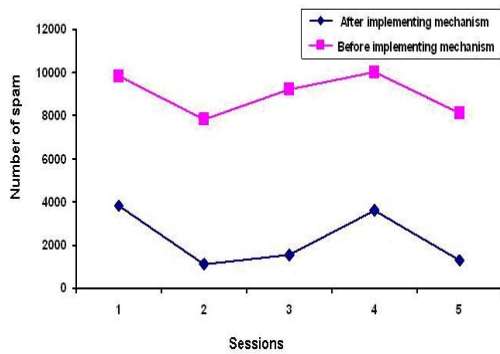
Figure 5. Defense Mechanism effects

5. Conclusions

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 experiencing 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 help to stop the possible DDoS attacks caused by spam. But fine tuning of filters mentioned in our mechanism prevented DDoS attacks through spam. The content filters clogged 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 educated users are responding well to this kind of attacks, the attacks avoided in an efficient way. The policies prevented the spam mails by utilizing policies of using signatures, no bulk mails, and the limitations of usage of group ids. Last but certainly not the least, the logical solutions to these attacks plays an important role to stop the attacks. The experiments show the effectiveness of SURBL to filter the 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 past six months.

6. References

[1] Jae Yeon Jung, Emil sit, "An empirical study of spam traffic and the use of DNS Black lists", ACM SIGCOMM Internet measurement conferences, Italy, Oct 25-27,2004, pp 370-75.

[2] Anirudh Ramachandran, David Dagon, Nick Feamste, "Can DNS-based Blacklists keep up with Bots", CEAS 2006, CA, USA, July 27-28, 2006, 1-2.

[3] Guangsen Zhang, Manish Parashar, "Cooperative mechanism against DDOS attacks",JRPIT 38,1,Australia, SAM 2005, pg 86-96, June, 2005.

[4 Anirudh Ramachandran, Nick Feamster, "Understanding the network level behaviour of spammers", SIGCOMM 06,Pisa, Italy, September 11-16,2006, 291-302.

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

[6] Ben Adida, David Chau, susan Hohenberger, Ronald L rivest," Lightweight Signatures for Email", DIMACS, 2006, USA, pp 93-99.

[7] David A Turner, Daniel M Havey, "Controlling spam through Lightweight currency", ICCS-04,HI,USA 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", CEAS-05, CA,USA ,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 .pp 47-58.

[12] Taughannok networks, "Technical response to spam", 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/

[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 http://spamassassin.apache.org

[22] SpamCop http://spamcop.net

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

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

[25] spamhous under attack http://www.virus.org/news/spyware/spamhaus-survives-DDoS-attack.html].

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