Volume 2, No. 5, May 2011

Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

MULTIHOMING ARCHITECTURE USED IN ATTACKING MAIL AND WEB SERVERS

(Role of Multihoming)

Kewal Krishan Sharma*[1], Dr. Rakesh Dube[2]

[1]Research Scholar, Mewar University, Chhitorgarh, Rajasthan, India
Email: kewals@rediffmail.com
[2]Department of Mathematics, Faculty of Science, Jazan University, Jazan, KSA
Email: duberakesh@hotmail.com

Abstract: Since the bandwidth is going cheaper and Web is increased rapidly, the number of the computer attached with world wide network is increasing dramatically. Multihoming is involved greatly in spreading information all over the world in no time. Multihoming is also going to cost a huge lose of bandwidth since much of information is traveled by the network either have no use, or repeated or virus codes. Much information is gone to be lost, when machine is get to be either cleaned or get to be formatted. In net shell, such information consumed lot of capabilities network and available bandwidth just for nothing. Here we have tired to show evidence on basis of real incident which we faced at our organization.

***Keyword*:** Distributed Multihoming Attack, bandwidth, Distributer Attacker, DDOS, Email Flooding, Multihoming Architecture.

INTRODUCTION

Ajay Kumar Garg Engineering College is a number one college in the NCR (National Capital Reason) and it is also rank one college in UP Technical University. It is located on National Highway no. 54. College is connected with outside world through Fiber optics and Radio link. The college has its own website www.akgec.org with running own mail Server which is based on MS Server 2003 and Microsoft exchange server. In between it started behaving mysteriously. Keep this in mind and other such incident occurred recently, to accomplished such attack; extensiveness of the intensity can be achieved by help of **Multihoming Architecture** [MA]. Very recently we have seen that how Julian Assange [1] had gathered the information from the secure links of US cables and made them available to rest of the world. In counter to avoid such websites, the American started bombards the *www.wikileaks.com* and other known resources of wikileaks, which USA believe that it belong to them. We have noticed that in such attacks the **Multihoming** [3] is playing great role. Multihoming provide the opportunities to hacker to attacked the network from various routs and node to intensify the effects and keep attacking from some other sources even some of their hosts are blocked and banned at targeted networks. The purpose of writing this paper is to distribute the knowledge about attacks to those, who are facing such problem in there networks. This is also helpful for those, whom network is not coming in the knowledge of hackers right now and may not be targeted yet, but likely to be attacked in future.

PROBLEM

Our problem was that web server which hosts our website and Email accounts started functioning unusual manner. There was a problem of generating lot of junk mails and many reputed mail servers like yahoo, Gmail and Rediffmail server started rejecting our mails. Any mail sent to these mail severs bounced back recipients server had given various reasons not to accept the mails. Our graph of bandwidth showing continues uploading and downloading. Soon we realized that our whole system had messed up. Our website become unable many time. Our server often restarts. Exchange server pending mail queue having thousands of undelivered mails.

ANALYSIS

By seeing that our bandwidth chart we found that it show continue upload and download even in those time also that at which we are pretty much sure that there should not be any activities, for instance in night 3 o'clock. This confirmed that some unknown activity is going on. Sometimes we found that the bandwidth consumed up to 4 to 5 Mbps by the server. Our one problem was that we have to analyze the source traffic where this traffic coming and going to, in our network, since our network is big network of around 1000 computer and having Wi-Fi and wired network. This network has hostel network and college network. Fortunately since beginning I had created two separate physical networks, one for College and for Hostel. Later on Wi-Fi and Hostel we mixed together. This network is spread all over the campus and hostel.

When analyzing the situation we found two major area of problem. First that our mail server was producing unsolicited mail in huge amount and Second our web server was targeted by several attacks. One of them was DDOS [4] attack and several attacks to try to force login and break into attack. We start comparing running processes of the server and comparing with some new installed server a number of processes are running and they could not be connected to known application, which were running on the servers. Some of the mysterious files are as below:

unwise.exe
unwise.exennezta388.exe
tbeza127q.exe
nnezta388.exe

Since lot of mail going to well known servers which were unsolicited and junk, they black listed our domain. This caused our authentic mails are bounced back from these server like Yahoo, Gmail and Rediffmail etc. We found that there were number of chine's site with multiple real IP were involved in this attack. While analyzing the back rout trace with help of command **tracert**, we found flowing observations.

1. The many attacking site were controlled be the Control agent, which uses to monitor the acceptances and relaying of our server. This is done by bouncing back the emails from college server. It is also monitored by that same mail was relayed to itself. If it does not reach for few hours and days, that mean we have blocked that IP address. So the control Agent initiates the command to those subordinate attackers who have not been yet blocked at college server. The subordinate agents are two types.
   a. One those they are deployed by the attackers directly.
   b. One those client node which are normal office computers or organization servers, but they are infected by worm or malicious software code install by remote access. Such computers indirectly start working as attacker. They often remain in dormant states, but become active on instruction received from control agent.
2. Our server running many unknown or mysterious process, few already state above.
3. Our server starts sending infectious mails to unknown address, which may causes infection transmissions to unaffected nodes all over the world.

By breaking the problems in pieces we found that the, we have to solve flowing problems.

1. That, why severs are uploading and downloading unknown data continuously, how to stop this.
2. Our bandwidth is not clean. Even with communication with our ISP it has been found that they have no control over there and issue remained unsolved.

The flowing DOS based tools are very important in case the widow based visual **Task Manager** is failed to load in memory since running virus process kill that instantly.

1. Tasklist.exe, Killtask.exe
2. Ping
3. Tracert
4. Nslookup
5. netsh
6. Various packet Sniffer tools

The system in which the attack accomplished from different computer to target computer we termed it **Distributer Attacker** and **Distributed Attacking Domain (DAD)** is set of such computers. A DAD can be spread over single network or may be spread across continents. There may be one DAD or multiple with single intention or may be individual intention. Know a days many research and advertisement companies are also involved in this area to propagate their information or to collect data secretly. To avoid such attack we established following concept. There should be a module which should attached it self at above network layer to monitor the incoming packets. If connected port / application is same for number remote computers it may be a multihoming attack. We created small routine and detected it and killed that process and got relief.

If such activities continued for long time it should be registered in network log file for later analysis and such packed should be dropped or blocked.

After analysis deep packet inspections that some structure of the packet was same in the many packets, but surprisingly they were sent from different remote machines. From reverse Arp analysis we found some packet from good website. We did not assume that these website are doing intentionally doing such activities. When we found that our mail server also sending many mail too many websites, which were unknown to us. We found that following architecture was implemented. We know this is a DDOS (Distributed Denial of Services) attack whose architecture is as given in fig. below.

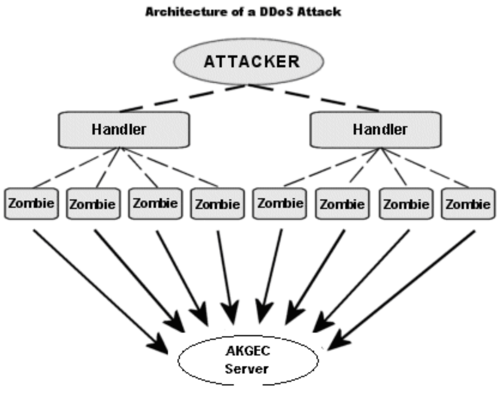


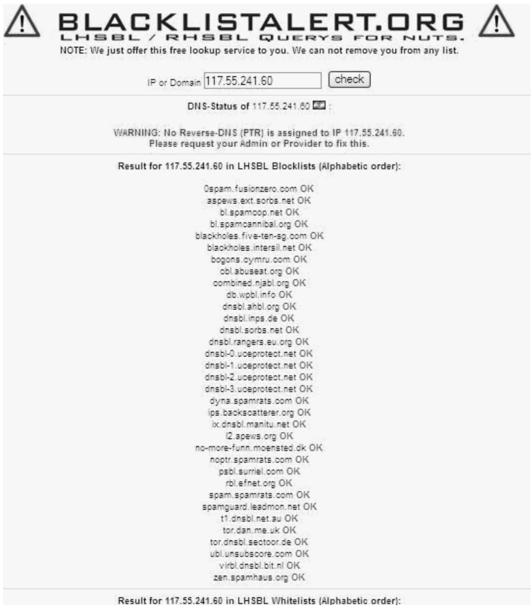
Fig. 1

DISCUSSION AND SOLUTIONS

We installed various Anti-Viruses software and try to control the situations. We found that some virus scanners doing something and some virus scanner doing other things. But none of them does not have full controlled on the situations. We also tired to ban some IP addresses on the server to block the emails from those IP. This help temporarily. Since the packets come from lot of different remote machines, blocking IP did not serve much. We reduced the available bandwidth to server avoid the consumptions of whole bandwidth of the college. It was clear the available bandwidth was enhancing the effect of attack to sever and to the other target machines.

As a solution we created a task list of process of window 2003 server of a fresh system. Than we created a script which use to run every few minute and compare task list of process with a fresh process list of process. Any new unknown process if activated, first it kill it and than log in another file for a record, we called it Terminated Process Log file (TPL). After sometime system administrator carefully check killed process in TPL and if Fresh list needed to reconfigure it updated it manually. This way, we become able to control the unwanted process to be activated.

Soon we found that our system started consuming less computer resource and organization main bandwidth. In our Mail Exchange server we stopped relaying mail messages which are not generated from our trusted users and our trusted IP address. This way we come out of the chain of E-Mail based Distributed Multihoming Attack.



```
BLACKLISTALERT.ORG
LHSBL / RHSBL QUERYS FOR NUTS.
NOTE: We just offer this free lookup service to you. We can not remove you from any list.

IP or Domain 117.55.241.60 [check]

DNS-Status of 117.55.241.60 :

WARNING: No Reverse-DNS (PTR) is assigned to IP 117.55.241.60.
Please request your Admin or Provider to fix this.

Result for 117.55.241.60 in LHSBL Blocklists (Alphabetic order):

0spam.fusionzero.com OK
aspews.ext.sorbs.net OK
bl.spamcop.net OK
bl.spamcannibal.org OK
blackholes.five-ten-sg.com OK
blackholes.intersil.net OK
bogons.cymru.com OK
cbl.abuseat.org OK
combined.njabl.org OK
db.wpbl.info OK
dnsbl.ahbl.org OK
dnsbl.inps.de OK
dnsbl.sorbs.net OK
dnsbl.rangers.eu.org OK
dnsbl-0.uceprotect.net OK
dnsbl-1.uceprotect.net OK
dnsbl-2.uceprotect.net OK
dnsbl-3.uceprotect.net OK
dyna.spamrats.com OK
ips.backscatterer.org OK
ix.dnsbl.manitu.net OK
l2.apews.org OK
no-more-funn.moensted.dk OK
noptr.spamrats.com OK
psbl.surriel.com OK
rbl.efnet.org OK
spam.spamrats.com OK
spamguard.leadmon.net OK
t1.dnsbl.net.au OK
tor.dan.me.uk OK
tor.dnsbl.sectoor.de OK
ubl.unsubscore.com OK
virbl.dnsbl.bit.nl OK
zen.spamhaus.org OK

Result for 117.55.241.60 in LHSBL Whitelists (Alphabetic order):
```

Figure.2 After the control

After some time our Exchange Server delisted from all reputed mail server since there is automatic mechanism to remove the name of Server from block list if it has not generated such unsolicited mail more than one month. Still the stream of the incoming unsolicited mail is coming in our network but they are not relayed further from our network. We expected soon it will be reduced to further a minimum.

CONCLUSION

We found that creating continues stream to a single node is not very difficult in this scenario of Multihomed World Wide Web. Multihoming can be achieved very easily and can be generated huge data in no time. There is some process in the computers those are capable of running all the time in computer doing nothing. Such processes are capable to provide the control of computer to remote system and give a path to establish a peer to peer connection at any time. They are capable of allowing hacking computer to down load new set of programs to host computer and run when ever the new program completely downloaded.

During controlling the bandwidth with various capacity we found that as we increased bandwidth to server the effect of the attack increases which causes the degradation in performance of the server as the below fig. show

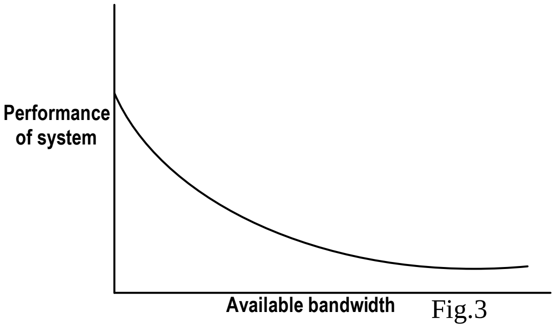


Fig.3

We noticed that the virtual memory continuously going consumed and system went down sharply down. Even server having 4GB memory, lot of memory consumed. It is noticed lot of TCP/IP connection established with no of remote machine, this all become possible due Multihoming pattern. System performance degradation due to multiple connection, server becomes non responsive to Web pages demand from the web. Sometimes information seekers feels that our website is down and they are not able to get website pages.

Future scope of the finding is that, there will be a great demand to handle such Distributed Multihoming Attack. Remote attacker identification is very important, blocking and clearance from the active network is required lot new software and hardware implementation. This issue will require new research and algorithms. Since a huge channel lose and resource performance already has been taking place, it is very much required a collective efforts has to be done otherwise the web will be also suffer a lot of traffic congestion due to non productive reason.

By analysis we traffic packets we found that most of the packet are junked and related to some conman IP addresses related and we assumed they are from Attacking Domain. The fig.4 clearly indicates.

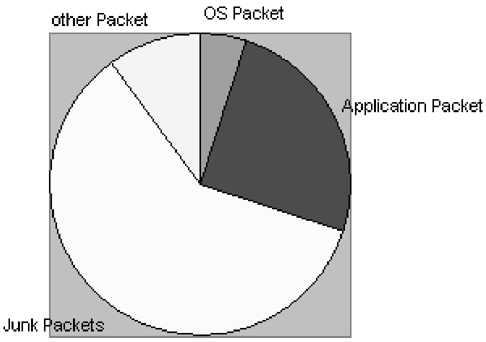


Figure.4 Losses due junk packets

Since Multihoming is only way to create number or routes from source to target node and able to consume the capacity of network. Multihoming is capable to use distributed capacity of network. Some network performs well and some do not perform excellent, reason may be anything, but Multihoming architecture is capable of consuming any capacity available in network. This is good in response to good manner, but creates very adverse effect in the network if used with malicious intention.

REFERENCE

[1] Dec 20, 2010, Outlook Weekly Magazine, www.war.com

[2] http://www.msexchange.org / tutorials / Mail_Relays_Enhance_Exchange_Security.html

[3] Lixia Zhang, An Overview of Multihoming and Open Issues in GSE, IETF Journal, Vol2, issue, Autumn, 2006.

[4] Rocky K. C. Chang , IEEE Conference Paper on " Defending Against Flooding-Based Distributed denial of Service attack: A Tutorial"