AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Dynamic Botnet Defence Mechanism For Malware Threat Protection

[1]M. Kempanna and [2]Dr.R. Jagadeesh Kannan

[1]*Research Scholar, Department of Computer Science & Engg, Karpagam University, Coimbatore.*
[2]*Professor, Department of Computer Science & Engg R M K Engineering College, Chennai.*

ARTICLE INFO

Article history:
Received 8 August 2014
Received in revised form
12 September 2014
Accepted 25 September 2014
Available online 1 November 2014

Key words: *Network security, dynamic method, Malware threat, Botnet defense*

ABSTRACT

Botnet defense is the mechanism of confining the impact on the worm or threat against its further impact. It is established and proposed in various ways either by existing, secure way of protecting against the initial attack mode or by stopping it from further layers of attack . However this proposal will acquaint a dynamic method to analyze the initial survey and protection layer by clustering nodes with master and slave subject. This method gain the qualitative method to slow down the initial impact on signatures matching against the worm nature and it will completely stop the spreading nature using antispam shields against it. In this paper, the algorithm to detect any bot will be partially based on biased nature of intrusion detection systems. However Network (IDS) start spreading messages of the bot nature which also leads to False Alarm. This paper will also critically discuss about, how it's avoiding the old messages exchange of master and slaves.

To Cite This Article: M.Kempanna and Dr.R. Jagadeesh Kannan., Dynamic Botnet Defence Mechanism For Malware Threat Protection. ***Aust. J. Basic & Appl. Sci.,*** *8(16): 18-24, 2014*

INTRODUCTION

This paper proposes a structure to approach the bot and its defense in a multi-hosting environment clustered in a network. A classical bot is simply a worm which is spreading in a service running network or into a DMZ network. Further this will usually enters through a specific users machine's IP (victim BOT) and it will either enters automatically download in the machine by a fake download link or from an untrusted website. An Usual nature of a BOT is to start fetching the information from its intend work or it might lead to a Denial of Service attack (DOS) to a service running environment. However the attack strategy is handled by IDS or passively through a honey pot mechanism. Survive from a secured network is not at all useful to defense against the BOT impact. Because typically worm either sends information from the victim machine to the master or it will start its impact to ruin the service. A master and Zombie method will play the same role as BOT and its master, once it enters in to the Network a said mechanism should prevents it from all of its further work, but that isn't happening. Clearly this mechanism will introduce the dynamic way of protecting a bot from further impact and its initial attack by signature based detection, further even in this detection technique the worm signature will change dynamically. Henceforth signature based detection will not help, even if it not in the proper update from database of Anti spamware defense mechanism. This method introduces a module to defend against the worm using a architecture comprises of master node, slave node, with message exchange about the worm based on operating system Kernel, database to maintain the worm structure and to avoid fake messages between master and slaves. Many methods discussed the bot defense by either centralized or structural methods, but there is a proportional idea for centralized suffers and network based intrusion detection system consequences. Before to explain the defense, normally a bot will works on the following ways. Bot is prepared by a master who uses it as a Zombie in a outside network namely through internet. It enters into the DMZ or a vulnerable system through an email or any other victim machine. However there are plenty mechanism envealed the bot defense which is discussed in this literature review of this paper in the chapter 2.

Literature Review:

A. Structural Approach:

Bot method based on the structural approach gives architecture with nodes and an setup to liable to protect the bot impact. However the honey pot mechanism uses the same method as a structural approach, either it using sandbox technique to dig deeper analysis about the worm and its structure. This approach will not help to

Corresponding Author: M. Kempanna, Research Scholar, Department of Computer Science & Engg, Karpagam University, Coimbatore.
E-mail: kempsblr@gmail.com

defense against the worm proactively but not much staggers in the detection mechanism. Also it never compromise the overflow technique used against the allotted buffer in it, because Bot in a service running environment will make such a difference for any analysis and make compromise the environment using DOS attack. In relation with the structural environment honey pot gives an analysis about the worm and its impact with limited resources but it doesn't give the complete defense for the worm layer. Structural approach is not a successful in case of protecting a worm from issuing commands from its Bot master. It influence largely against the distributed method which is based on proposed method introduced in this discussion, specifically an IDS is also an distributed environment which defense almost all type of intrusions in a secure network.

B. Distributed Network:

When it comes to the discussion of distributed network, this must specifically discuss the nature of Intrusion detection mechanism and its types. IDS are a well secured architecture plays a vital role in network security and BOT net defense strategy. It is classified into anomaly based which holds based on traffic profile against outside the firewall or it after enters inside the firewall. However these methods also based on traffic profiling and flow of traffic. However this might gives some proactive detection, it never discussed the traffic from anonymous users who are always using the Zombies from BOT masters. Hardening against the system and its supporting software will also helps but not gives a user free host environment. Whereas in host based method detects internal and external bot with the scanning ports of internal and external devices. But it is not comes in proactive methods of structure and successions. It analyses the behavior based on the bot nature using its command exchange method. Again it falls in the reactive method. Severely IDS would help to assists the BOT defense but more literally this mechanism needs more independent mixed part of Distributed environment than Intrusion Detection System. Network based method composes an architecture that is more similar to the methods of implementation used in this approach, however here survival adapts to the Centre point of failure. As a biased nature of IDS, every node sends information about each other every two minutes which is another method to defense against Bot and its spreading nature. The Nodes synchronization with each with interaction is important in every network based IDS.

C. Honey Pot:

A simple honey pot will be a better solution?, Not at all because defining a honey for a versatile ambience of a Bot net could not be that much easy. A more harden form of a honey pot mechanism will have a sandbox which will handle the worm and its history by matching with a database. However it might also have white box and black box testing which is similarly used in software testing platforms. But it is slightly differed in this concern by the following. The white box in Honeypot nepenthes platform fetch the worm first and puts into the white box, where it is totally different in original software testing and then it will collect information using Sandbox. After that the analysis will further continues into the vault storage system which is also another method of filtering. Here is the summary of all mechanism clustered together in analysis worm and filtering it when it is initiated by a bot master. As a conclusion, honey pot mechanism will partially fit in to the defense method but will never fits into these botnet defense mechanisms. Clearly when an IDS and Honey pot combined in a vault surfing mechanism against a bot will be helpful and never easy when it making together of this two. Web surfing from an anonymous part of world is also an easy method, using an anonymous web surfing tool. It is simple as that like profiling and cookies to capture user and his anonymous role. This is further fairly discussed in next two sections as follows.

D. Cookies Collection For Anonymous Bot:

As the definition stands the bit of information retrieve here is transmitted not through the secure channel. For instance if a user tries to surf a proxy website and try to browse the popular video surfing website say YOUTUBE means, proxy website sends the cookie in the name of youtube to the browser that user actually worked on, provided the user web proxy site is in http not on *https* .however cookies are the only assertive proof to collect the information about the users session, furthermore cookies are stored in the non volatile memory of system which user uses to browse. When a user browsing the web, the session is carried in the following two ways. Firstly the request is made to the web server with the ip address of the user machine. Instead in proxy, user request is carried by the proxy and it response back to the client machine using get method. These cookies are called as persistent which will be lasting for maximum of a year. So the weight of evidence would suggest that instead of tracking entire session, dissolute the http protocol and get method will give fair state of user cookies. However cookies set by the normal characterized websites appropriate to the user actions like the following when searching a file or content, clicking an image, open a link etc. furthermore proxy websites of accustomed home page with a search field which returns an user expecting another webpage. Hence obviously cookies must set by proxy website every time when user typing a URL, as a result such cookies contains only web address information or at least the unique name of the website.

Australian Journal of Basic and Applied Sciences, 8(16) October 2014, Pages: 18-24

E.User Profiling:

The user profiling is the way of maintaining the user records to identify whom they are claimed to be?, the components of user must be updated in the server when the clients first enrolled for instance workers belong to same organization individually have an authentication credentials to access the machines inside. The profiling data contains email address, phone number, including user credentials. This is matched when user was successfully surfed out from a session and every ip packets must mirrored and stored in a server database.

F.Authentication:

Authentication policy for every secure infrastructure is a valid and conspicuous key idea. When clients try to access an machine he must be authenticated and a session token is granted based on the user policy he /she holds like Kerberos protocol. Unless it mutually authenticate server and clients, here the idea is to grant permission to user furthermore with the session token. So that, no user cannot repudiate back that the certain proxy website is not browsed. This concept of coupling active directory service closely with Kerberos debuted in windows 2003 operating system (Zin *et al*., 2012). Whereas Active Directory Service maintains user profile and Kerberos sustains authentication for client. Most of the e-commerce websites authenticate the customers based on the user credentials and trust is made by trusted third party like key distribution which mutually authenticates both the clients and server. By the same clients of inside domain are authenticated by server and correspondingly they can access resources.

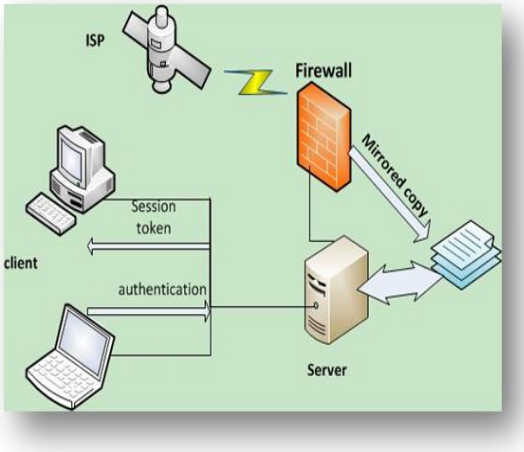

Fig. 1: Authentication system

II. Problem Statement And Attack Discussion:

A significant literature review is done on the various botnet defense mechanisms and summary of implementation in this part of the paper. Though it survives to discuss the traffic flow, the recommendation suggested as making a defensive method based on http traffic flow using port and blocking in further impact of spreading. Xiaolong Ma *et al*. (2012) proposed an method for eliminating link and node strategy for complete rid of bot behaviors from nomadity between peer to peer links, however this process eliminates the further spreading problem but elimination technique is simply like isolating the machines from network which wouldn't help disaster management between nodes. Further it is not critically analyzed the rate of elimination and choosing of node to eliminate.

Various technologies are involved in technically evaluate the basis methods (Raghava *et al*., 2012). Another method proposed by Meisam *et al*. (2012) defines a new generation of mobile botnets to detect the raising span of bot in mobile devices through network connections. In that paper mobots (mobile Bots) behaviors and impacts of both botnets and malicious activity, however proposed system is not fully converged as compared to existing methods (Chia *et al*., 2012). Malicious behaviors will change from time to time like signature. Further the Mobots agents are proactive which results in overwhelm the resource using by the mobile devices. Moreover researches describe the monitoring bot activities based on visualizing monitoring tools, which assists to monitor the behavior of bots instead of protecting it from feature extend (Alireza *et al*., 2012). However this paper managed to critically analyze the current behaviors and introduced VTM but failed to describe the robust way of proactively protecting from the threat. Similar reference takes into consideration because it actively reports the impact and vulnerability of bot pc. The study proposed by Wu *et al*. (2012) discusses the nature of botnet design parameters, three types of modules to handle the proposition of malwares further up to deletion. However this wasn't discussing the false alarm rate of detecting the same malware and repository to retrieve or match it back.

Australian Journal of Basic and Applied Sciences, 8(16) October 2014, Pages: 18-24

Botnet detection is classified in to network based and signature based method which added as service method to the botnet mechanism (Hossein *et al*., 2012). Pijush *et al*. (2012) introduced an SVM tool to capture the extract the raw data using a Perl script. Based on the hierarchy of data set extraction, each flow can be further analyzed to exhibit a bot free network. Further flaws will only occur in that proposal when the malicious nodes send encrypted form of data and signature changing. SVM classifier tool was used to extract and produce the analysis report based on raw data. All above methods similarly handle the analysis protocol between peer to peer model, similarly Deepali *et al*. (2012) introduces kademlia evaluation method and produces an simulation for demonstrate the bot nodes about the issues been raised by the malwares in the network, further this paper is taken as a asses model for the proposed method going to introduced in this research. This support gives to achieve the botnet with dynamic defence alongside of learning node behaviour. Entropy method for the same p2p based on user behaviour was introduced in Jin *et al*. (2102), but enough percentage of analysis proven that dynamic changing malware or certain threat is immeasurable against the botnet nature.

III. Proposed Method:

i. Monitoring:

For a method to be complete in a network, it should follow a complete set of procedure like FCAPS (Fault Configuration Accounting Performance Security). Before any Fault occurs, a proper monitoring of nodes to be exists using some famous platform dependent network protocol is needed. Here it might be several which is using DCOM or SNMP, however for this model gets its complete structure by using Simple Network Management Protocol. If network changes are required, maintenance personnel will need to make modifications to these areas in order for a user to operate properly. The SNMP support lets anyone manage network security, which helps to find and solve network problems. The SNMPv1, SNMPv2 and SNMPv3 are three major versions of network protocol released in various time to support an initial fault management of this network model. User must configure a SNMP to monitor the health and defense against BOT. It uses GET/SET messages to for collecting statistics and traps for collecting events. SNMP lets an NMS (Network Management System) like the Bot remotely collect reports and traps using software's. The traps are SNMP notification sent over to the specific NMS hosts, whenever an event occurs. The configured SNMP agent generates traps for bot events like, when event such as worm enters in to the network etc., the SNMPv3 security for authentication and authorizations for network support.

ii. Nodes and Services:

SNMP service comprises to three nodes which are as follows, the major three components in regards to the protocol managed devices, agents and network-management systems (NMSs). Managed devices are a network node that contains an SNMP agent and reside on a management network. It will collect and store management information of worms, the info's are service affecting worm either its vulnerability it uses to enter, impact it will make, whether it enters earlier into the network . These devices may be routers, servers, switches, hubs, hosts and printers.

Agents an agent is a network management software module that resides in a managed devices. However similar methods like honey pot needs nepenthes are platform and sandbox. Software modules performing a crucial role in a boot management of a bot defense mechanism. Here an agent must have local knowledge of management information and translates the information into the SNMP-compatible form.

Network management Systems: An NMS executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for the BOT management. One or more NMSs must exist on any managed network. Several companies provides NMS application on the market today; Hewlett Packard's open View, Trivoli's TME If you are Enterprise console, computer Associates Unicenter and Sun microsystems' Solstice just to an name a few.

iii. Management Information Base:

The management information Base is a collection of information organized hierarchically. They are two types of MIBs: scalar and tabular. Scalar objects define a single objects instance whereas tabular objects define multiple related object instances grouped in MIB tables. MIBs are collection of definitions which define the properties of the managed devices (such as router, switch etc.,) each managed devices keeps a database of values for each of the definition written in the MIB. As such, it is not actually database but implementation dependent. Each vendors of SNMP equipment has an exclusive section of the MIB tree structure under the control.

In order for all of this to be properly organized, all of the manageable features of all products are arranged in the tree. Each tree has organized number of Bot nature and its structural approach of attacks and completes the entire bot and worms' nature is organized and staggered entirely.

Australian Journal of Basic and Applied Sciences, 8(16) October 2014, Pages: 18-24

iv. High Availability of nodes and BOT defense:

Two Nodes are defense against each other using a redundant cluster. The redundant peers are getting to each other and are referred to individual as nodes. During the failover, the standby becomes active almost immediately but it should takes of 500 ms or less than that of all process to come up and for traffic of Bot will carry out by the master service. The bot defense with high availability cluster to work around the method for quick process and without failure. Such service affecting method survives overall defense security of network both a bot and its Bot nodes with an active master and passive slave mechanisms

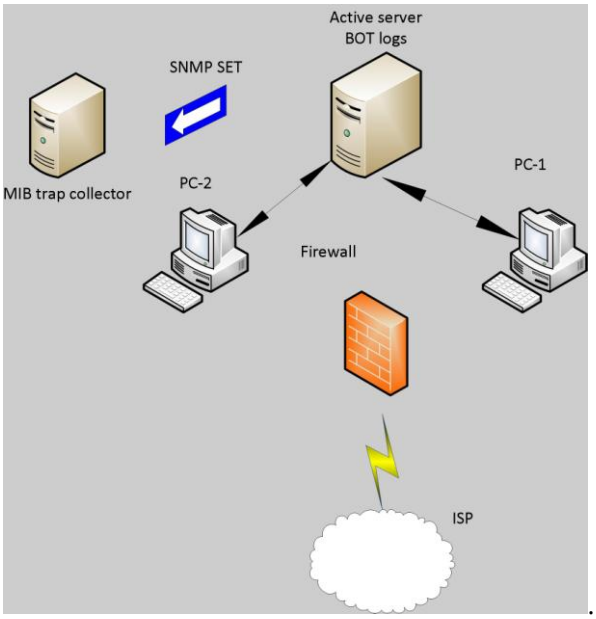

Fig. 2: Bot defense mechanism

This mechanism and the bot defense flow have an enough structural approach and non-service affecting architecture. However every mechanism must need a improvements as it always structured with enhancements, therefore there is an service tuning architecture gives a extra flow with few cryptographic encrypted message exchanges. Normally this mechanism never need a key exchange mechanism because, such service strongly recommends a key database with lot of trivial methods and terminal mechanisms. This method uses as same as the previous architecture comprises of SNMP with a minor difference. SNMP traps and collection method atomized here with encrypted exchanges, nevertheless dematerialized zone never support a big infrastructure, such as router managing a machines and server components. Modern technology supporting cloud servers and compatible IPV6 service and IPv4 enabled architectural systems. This will enhance some architecture ease and in terms of security perspectives.

1. However the proposed method comprised a defense enabled system with log collection machine and a machine will process such service by a simple SNMP service definitions. But service defense supports flow of messages between affected nodes i.e., BOT's but any service and security related architecture will compromise a security flaw.
2. Necessarily a bot defense against a malware uses either IDS or honeypot with a sandbox, here this method Use proactive way of collecting logs against affected machines and it should be processed by a master with high available secure network.
3. Therefore advancement in the proposed method could be a solution will be the SNMPv6 server for exchange the bot messages will speed up the process and also services the message mechanism. Here an automated message can be initiated by bot affected machines in a machine which is software installed to send initial message about bot ideas and services.
4. This method improvement is advanced against IDS (network based) in the following way. A network based IDS host will send messages against each other and it is already discussed as very complex to surf the message against each and it will also result in a false alarms. This method excludes some common complexities found in IDS and some proposed method for bot defense just like it eliminates the messages passing replication using two different un-identical machines.
5. It also eliminate the process of slow service exchanges Using SNMP and also eliminates some false alarm rate towards the improvement of Bot defense mechanisms. Structural approach of an enhancement to this architecture with an automated exchange when a host initially detects a bot alert using Simple Network management Protocol.

Australian Journal of Basic and Applied Sciences, 8(16) October 2014, Pages: 18-24

The true positive rate (TPR) is used to measure the proportion of rightly detected attacks. The false positives (FPs) counter represents the amount of wrongly flagged as malicious. Both the TPR (in proportion) and the FPs (absolute value) are computed on a time based window basis. An alert may be generated (true or false positive) or not (true or false negative), for each rule, at the end of each window detection. Due to that, evaluating false positives as a ratio is irrelevant. Since benign traffic is in majority, the false-positive ratio does not vary significantly in the findings. The comparison of the proposed dynamic method with SVM and entropy methods in terms of detection rate and false positive rate are shown in Fig. 3 and Fig. 4.

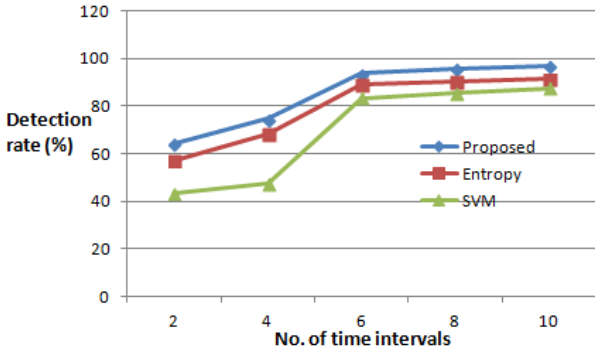

Fig. 3: Detection rate comparison

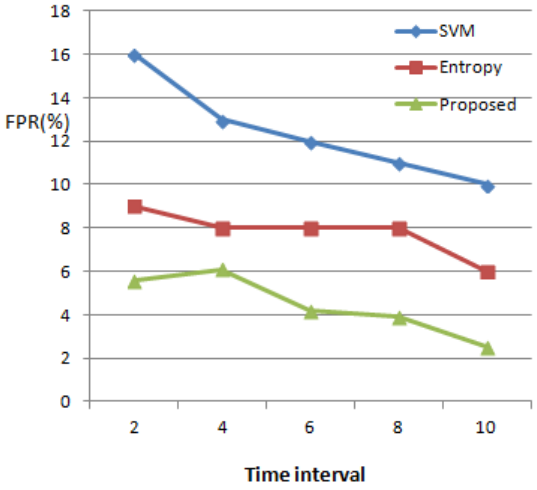

Fig. 3: False positive rate comparison

Conclusion:

The Service exchanges of BOT defense with all proposed method introduces an strongest bot defense but the bot master initiating such a malware threat is more and more versatile against many platforms such as data, network security and even common in highly available e-commerce security. But this Bot defense architecture introduces an advanced nature of defense against BOT by both proactive filtering and reactive defusing using all network enhancing elements such as DCOM in windows also a exchange management using SNMP's. Truly an terminating way of a Bot with its platform dependent security will never handle this in easy composition, technically any methods for such a proactive methods never be cost effective and never fits in to a budget of an organization, Any site nature of a architecture will support a certainness with listed amount of constant unit of structure but never commits to an organization economical critical. So as a event of easiness an bot Service always produces and well defense against but never gives validness in most changing technical network of unsecure world. And certainly a Bot master will never easily stop his/her nature of develop zombies against the unsecure world. As a conclusion, this method will be a good solution for the BOT nature even in the event of scarceness and it can be fine tune to the nature of enhancing its secure future will support a valuable bot free environment.

REFERENCES

chia mei-chen', sheng tzong cheng, ju-his, 2012. "International symposium on parallel architecture" – .Ieee conference, 10.1109/PAAP.2012.19 .

Rui sousa, nuno rodrigues, paulo salvador, 2012. Analysing the behaviour of top spam botnets, 2nd IEE workshop on smart communication on protocols and algorithms.

Meisam eslahi, Rosli slleha, 2012. Nor badrul anuar "Mobots : A new generation botnet on mobile devices and networks, International symposium on computer application and Industrial electronics.

Alireza sharestani, Maryam feily, Mona masood, 2012."visualization of invariant bot behavior for effective botnet traffic detection" IEEE conference on telecommunication.

Wu Xianghua, cao lijun, 2012. " Analysis and designof botnet detection system " , International conference for computer and services.

Tianzuo Wang, 2012. hiaumin wang, Bo lu"A study of strategy to restrain the C&C activities of structured P2P botnets".Computer security ESOROS IEEE conference held at chicago.

Pijush Barthakur, Manoj Dahal Mrinal Kanti Ghose, 2012. "A Framework for P2P Botnet Detection Using SVM", International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover.

Deepali Arora, Teghan Godkin, Adam Verigin, and Stephen W. Neville, 2012. "Assessing Trade-offs between Stealthiness and Node Recruitment Rates in Peer-to-Peer Botnets", Seventh International Conference on P2P, Parallel, Grid, Cloud and Internet Computing.

Jin Zhigang, Wang Ying, Wei Bo, 2012. " P2P Botnets Detection based on User Behavior Sociality and Traffic Entropy Function" School of Electronic Information Engineering IEEE conference.

Raghava, N.S., Divya Sahgal, Seema Chandna, 2012. "Classification of Botnet Detection Based on Botnet Architecture" ieee International Conference on Communication Systems and Network Technologies

Hossein Rouhani Zeidanloo, Mohammad Jorjor Zadeh, M. Safari, Mazdak Zamani, 2012. "A Taxonomy of Botnet Detection Techniques" Second International Conference on Computer and Electrical Engineering.