International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 103 - 107, 2015, ISSN:- 2319–8656

Malware Hunter: Building an Intrusion Detection System (IDS) to Neutralize Botnet Attacks

R. Kannan
Department of Computer Science
Sri Ramakrishna Mission Vidyalaya
College of Arts and Science
Coimbatore ,Tamilnadu,India.

A.V.Ramani
Department of Computer Science
Sri Ramakrishna Mission Vidyalaya
College of Arts and Science
Coimbatore ,Tamilnadu,India

Abstract: Among the various forms of malware attacks such as Denial of service, Sniffer, Buffer overflows are the most dreaded threats to computer networks. These attacks are known as botnet attacks and self-propagating in nature and act as an agent or user interface to control the computers which they attack. In the process of controlling a malware, Bot header(s) use a program to control remote systems through internet with the help of zombie systems. Botnets are collection of compromised computers (Bots) which are remotely controlled by its originator (Bot-Master) under a common Command-and-Control (C&C) structure. A server commands to the bot and botnet and receives the reports from the bot. The bots use Trojan horses and subsequently communicate with a central server using IRC. Botnet employs different techniques like Honeypot, communication protocols (e.g. HTTP and DNS) to intrude in new systems in different stages of their lifecycle. Therefore, identifying the botnets has become very challenging; because the botnets are upgrading their methods periodically for affecting the networks. Here, the focus on addressing the botnet detection problem in an Enterprise Network

This research introduces novel Solution to mitigate the malicious activities of Botnet attacks through the Principle of component analysis of each traffic data, measurement and countermeasure selection mechanism called Malware Hunter. This system is built on attack graph-based analytical models based on classification process and reconfigurable through update solutions to virtual network-based countermeasures.

Key words: IRC, IDS, Anomaly, Countermeasure, Denial of Service.

1. INTRODUCTION

Network security consists of the requirements and policies adopted by a network administrator to prevent and monitor various forms of intrusion and attacks on services obtained via Net[2]. To access the data over network, an efficient authentication is needed which is provided and verified by the administrators. The user gets user identification and password to get access to the targeted network. The network security encompasses all types of networks including private ones[9]. All types of transactions whether public or private such as government services, business activities etc need security for their data and other resources of a computer network. The Network security system secures and protects the net based resources. The proposed framework leverages hierarchical models to build a monitoring and control process to classify the network traffic data to the virtual machine to significantly improve attack detection and mitigate attack consequences[8].

1.1 Problem Definition:

Data and Network security is one of most important area that has attracted a lot of research and development effort in recent times, particularly, in the area of cloud data protection. The vital information of all types have to be secured against attackers to prevent from exploring the vulnerabilities of a cloud system and prevent them from compromising the virtual machines by deploying a large-scale Distributed Denial-of-Service (DDoS) system. DDoS attacks usually involve early stage actions such as multistep exploitation, scanning, and convert the virtual machines and do attacks through the compromised machine (zombies) which have been taken over by botmasters to hide from detection. In the cloud also, i.e IaaS cloud[2], the detection is difficult in case of attack with novel characteristics. This is because cloud users may have installed vulnerable applications on their virtual machines.

1.2 Botnet

A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be of any type such as taking control of an Internet Relay Chat (IRC) channel or sending of spam mail or participation in DDoS attacks. Botnet is a name constructed by joining the terms robot and network[3][4].

There are many types of attacks and detection systems with the malware help. The classification of attacks are as given below

- In DDoS attacks, various sources submit multiple requests to a single Internet based accessible point and overload it with fake request and prevent the point from accessing needed data For instance if a phone number which tries to connect to internet[1][9]
- Adware intrusion hides the original advertisements with fake ones on web pages
- Spyware is software which sends information to its creators about the activities of the users. Compromised systems exist in an establishment network can be useful since they possess information useful for the

organization. The valuable data are stolen by these spywares and misused by the intruders

- E-mail spam contain advertisements and malicious contents.
- When a false web traffic is generated for some gain it is called Click fraud [9].
- Fast flux is a DoS attack the botnet uses to hide the phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies.
- Brute is way of making remote machine services such as FTP,
- Worms. The botnet focuses on recruiting other hosts.
- Scare ware is software that is marketed by exploiting the fear of users. This kind of scare ware make the attacked computer as a bot and induce the user to buy a rogue anti-virus to regain access to their computer.[9]

An intrusion detection system (IDS) is an application program that monitors network and system functioning for malicious activities or policy violations and produces reports to a server which supervises it. Various methods are adopted to detect traffic which are suspicious in nature. Generally the IDS are classified in to two, namely Network based detection system (NIDS) and host based detection systems (HIDS). The Intrusion detection and prevention systems (IDPS) concentrate on identifying possible incidents of logging information about them and inform the attack attempts.

Types of Intrusion Detection system

1) Network Intrusion Detection Systems:

Network Intrusion Detection Systems (NIDS) are placed at a strategic point or points i.e in between the server to which the system connected and to the Internet. It analyses the traffic and matches the traffic that is passed on the subnets to the library of earlier attacks. On finding the attack it alerts the administrator[2][3].

2) Host Intrusion Detection Systems

Host Intrusion Detection Systems (HIDS) run on individual hosts or devices connected to network. A Host Intrusion Detection Systems scans the data and will alert the user or administrator of suspicious activity is detected. It compares the existing system files with the earlier files. If any mismatch is found it alerts the administrator. The example of the Host Intrusion Detection Systems are useful in the mission critical machines that are not expected to change their configuration. The HIDS (*Host Intrusion Detection Systems*) can be customised to the specific needs of systems.

Statistical Detection Techniques used in Intrusion Detection System

A. Statistical anomaly-based IDS

An Intrusion Detection System (IDS) which is structured on anomaly will monitor network traffic and compare it with standards. The Intrusion Detection System will find the deviations from the standards for the network and other parameters such as protocol, bandwidth and allied devices and alert the administrator or user when traffic is detected which is anomalous or different to significant level than the preset standard. However there is a possibility for False alerts even for a legitimate use of bandwidth if the baselines are not intelligently configured.[2]

B. Signature-based IDS

A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from identified threats. This kind of antivirus program detects malwares in this way only. The real problem is identifying the fresh threats and the signature for detecting that threat being applied to Intrusion Detection System.
Hence identifying new threats will be a problem [4] in this method of detection.

Problem Objective:

However, all the above threats fall in to the category of Botnet. This study proposes a new solution to mitigate the malicious activities of botnet attacks through a detection mechanism and gives a strategy for counter. To prevent attack on virtual machines which exist in the cloud, a multistage distributed attack detection system through the Principle of component analysis of each traffic data, measurement and countermeasure selection mechanism called Malware Hunter. This system is built on attack graph-based analytical models based on classification process and reconfigurable through update solutions to virtual network-based countermeasures. The proposed framework leverages hierarchical models to build a monitoring system and control process to classify the network traffic data to the virtual machine to significantly improve attack detection and to eliminate risk.

2. SURVEY OF LITERATURE

2.1. Detection of Spam Zombies

This study focuses on compromising of the machines which is one of the key security threats on the Internet. This technique is used in preventing various forms of security attack. The attack of spamming provides an economic incentive for attackers to recruit the large number of compromised machines, here the aim is to focus on the detection of the compromised machines in a network that send spam, which are called as spam zombies. The development of a good spam zombie detection procedure named SPOT by monitoring outgoing messages from network. SPOT is system designed and named based on a powerful statistical tool Sequential Probability Ratio Test. Additionally, the performance evaluation of SPOT using a two-month e-mail trace.

The evaluation studies show that SPOT is an effective and efficient system in automatically detecting compromised machines. For instance, among the given IP addresses which were observed in tracing e-mails, SPOT identified more than one quarter were connected to bots. Of these bots except very few could be confirmed independently and these few were with possibility for attack. Further the SPOT failed to detect only seven machines in the process of tracing. In fact SPOT out performed, other two detection

algorithms which used the method of comparing number and percentage of spam messages enter, efficiently.

2.2. Detecting Malware Infection through IDS-driven Dialog Correlation

In this study, a new kind of "Network perimeter monitoring strategy", was used to check the correspondence during the period of an infected system. Monitoring system is process developed to track the two-way communication flows between internal assets and external systems that match a state-based modeled on sequence of infection. It consists of a correlation engine that is driven by three malware-focused "network packet sensors", to find malware infection in various forms and activities and to prevent attacks on external systems

The Monitoring system finds such internal external system links and indicates that there is an infection in the local computer(s). The Monitoring system matches infection dialog model with actual infection, generates a report and lists out the relevant events and event sources that played a role in the infection process. The method of analytical strategy matches the flow of correspondence between the intra and the Internet. This contrasts the strategy to other intrusion detection and alert methods. Here the results are given using Monitoring system in both virtual and live testing environments and discuss our Internet release of the Monitoring system prototype. The monitoring system is made available for operational use and to help stimulate research in understanding the life cycle of malware infections.

2.3. Scalable, graph-based network vulnerability analysis

Well secured networks are also vulnerable frequently due to constant innovation by attackers. New combinations of exploits are innovative ways through which attackers do attacks. The researchers forth a multiple graph-based algorithms in the form of trees/graph attacks. The proposed trees/graphs consider all possible types of attacks to penetrate in to a system or network, using previous exploits also.

The latest approach uses a modified version of the model checker NuSMV as a powerful inference engine for chaining together network exploits, already happened. In this study the researchers argued that the method gave more data than actual need for analysis and its ability to handle bigger size of networks and they proposed a representation compact size and scalable.

They claimed that it was possible to produce attack trees from their representation with even more information for bigger networks, even when they if they do not go through attack tree. The claim of them stated that attacker can bypass backtracking. This assumption eliminated the need for analysis at higher level unnecessarily and made larger network within the reach of analysis.

2.4. MulVAL(Multivalue): A Logic- Based Network Security Analyzer

This study determines the security impact software vulnerabilities on a particular network, and considers interactions among multiple network elements. For a useful vulnerability analysis tool there are two factors to be taken in to consideration namely, the ability to integrate the given vulnerability specifications automatically from bug-reporters and the scalability with larger networks. They proposed to develop MulVAL, a overall framework to conduct the analysis of vulnerability on multiple hosts and multiple stages on networks. The MulVAL adopts Data log as the modeling language for the elements in the analysis in specification of bugs, describes the configuration defines rules for reasoning to find malware, getting permission of OS and provide model for privileges etc. They leveraged the vulnerability-database existed and scanned tools by expressing their output in Data log and feeding it to their MulVAL reasoning engine. The collection of information helps to analyze in a shorter span of time even for larger networks.

2.5. Scalable Optimal Countermeasure Selection Using Implicit Enumeration on Attack Countermeasure Trees

The constraints, on the basis of investment cost on security preclude a security decision maker from implementing all possible measures to counter. Present security optimization strategies based on analytical model do not prevail for the following reasons:

(i) No method provides an optimal security solution in the absence of probability assignments to the model.

(ii) When size of network grows, the efficiency of the tool decreases

(iii) The methods which follow attack trees (AT) normally do not allow for the inclusion of countermeasures On the other hand the non-state-space model (e.g., attack response tree) responses are modified in to state-space model and cause state-space explosion.

This researcher proposes a new AT paradigm and named it attack countermeasure tree (ACT) whose structure takes into account attacks as well as countermeasures (in the form of detection and mitigating attack events). They used techniques of branch and bound, greedy method etc to study multiple objective functions with goals such as minimizing the number of countermeasures, the cost of security of ACT and maximizing the benefit from implementing a certain countermeasure set in the ACT under various constraints. They formed every problem of optimization as an integer programming problem which also allowed them to find optimal solution even in the absence of probability assignments to the model. Their method of scales suited for larger ACTs and they compared its efficiency with other approaches.

3. METHODOLOGY

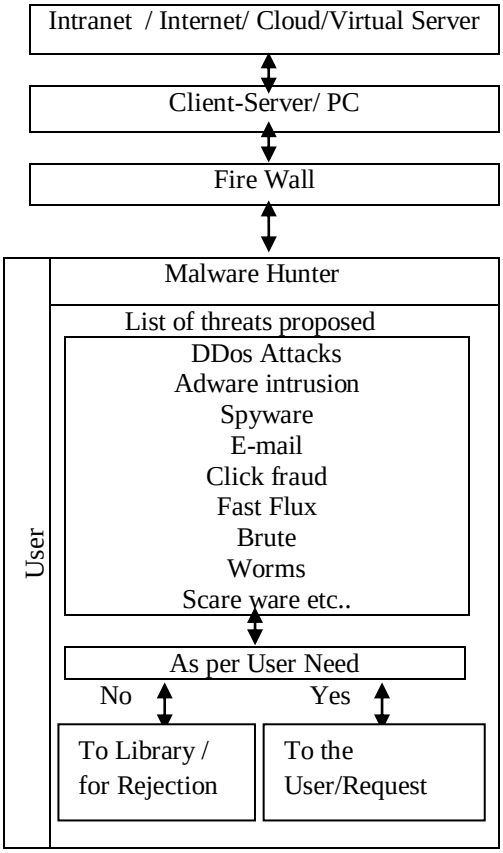

Fig 1: Architecture Diagram of the Malware Hunter Establishment of a Host and Network layer to monitor the Network

Host based intrusion detection [3] system is modeled to capture the attack to the host through monitoring and prediction process. In fig 2, the architecture for the proposed security model has been shown.

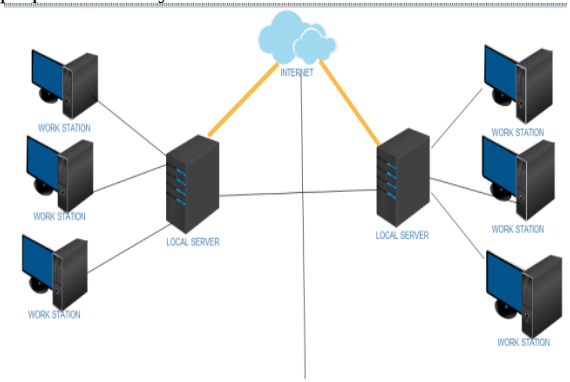

Fig: 2 Architecture of Network Based Intrusion Detection System (IDS)

Threats faced by the applications can be categorized based on the goals and purposes of the attacks. A through exposure to the forms and purposes of threats put a person in an advantageous position in detecting the threats and neutralize them.

The properties of attack and Identification of various forms of attack.

- Network performance is abnormally slow (when files are opened or access to web sites)[9]
- Non availability of access to a given web site
- Inability to access any web site
- Increase in count of the number of spam emails received—(this type of DoS attack is considered an e-mail bomb)
- Frequent Disconnection to Internet
- Denial of Internet access to the Net[10].

Denial-of-service attacks can also lead to problems in the network 'branches' around the target computer. For instance, if a router of a LAN and Internet is attacked, it may compromise all the computers connected to the Network. In case of larger scale attacks, Networks at regional level may be infected, irrespective of the intention of the attackers.

Procedure 1: Reading the File through Buffer Reader

Step 1: Start
Step 2: Create a File
Step 3: Copying the File & then it will compare with each node & Reading the List.
Step 4: Condition is checked, it's true it will attach the file in to buffer reader.
Step 5: If it's False then copy the file into Buffer.
Step 6: File will be monitored.

Procedure 2: Reading and Writing a file in Buffer

Step 1: Start
Step 2: Create a File
Step 3: Copying the File, Then it will compare with each node & reading the list
Step 4: Condition is checked, it is true it will attach the file into buffer writer
Step 5: If it's false, then malware type will be stored in buffer writer

Formatting the threat forms

Novel threats in the network and host system is difficult to identify due to the changing strategy of attackers. An efficient novel attack detection system has the characteristics of each event (i.e., the pockets of IP / the TCP connection) such as payload strings and induction of conditional rules which have a very low probability of being violated shall be framed[3][4].

Learning Rules for anomaly detection

1. We extend the network traffic model to include needed quantum of attributes and payload application.
2. We introduce a non-stationary model, in which the event probability (an attribute having some value) depends on the time of its most recent happening.
3. We introduce an efficient algorithm for selecting good rules for anomaly detection from a rule space that is exponentially large in the number of attributes.

4. RESULT AND ANALYSIS

The system against botnet and DOS attacks which are shown below. Most of the attacks shown with some evidence, so here the results are simplified and report the detections.

It illustrates how to dynamically add malware behaviors. In each system call concerned, we set up needed checkpoints and each of these check points is responsible for checking the behaviors belonging to the same operation with the support of a modifiable behavior list in memory.

The performance results provide us a benchmark for the given hardware setup and shows how much traffic can be handled by using a single detection area. Construction of a distributed model to scale up to a data center-level IDS is needed.

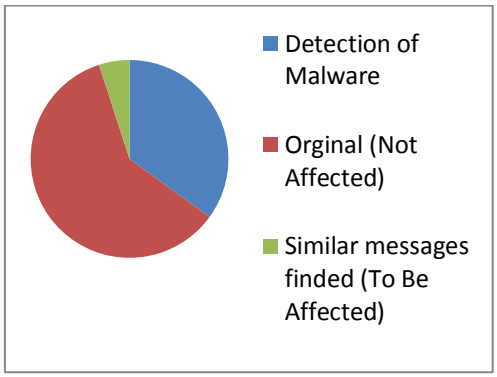

Fig 3: Detection Accuracy of the Malware Hunter Data Recovery process

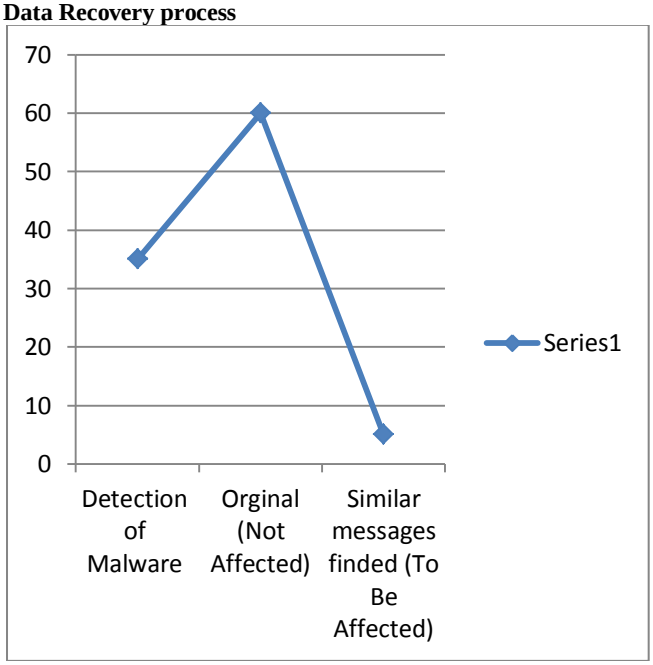

Fig 4: Rate of data recovery

5. CONCLUSION

The results show that the Detection of Accuracy of the Malware hunter in multiphase distributed vulnerability detection through the Principle of component analysis. Each traffic data is under the dynamic attack evolution capacity and countermeasure selection mechanism called Malware Hunter which uses graph-based analytical model for its formation, uses the classification and reconfigurable process against update solutions to virtual network-based counter measures. The classification is done using the principle component analysis to establish the efficient detection mechanism against various types of attacks. The modeling parameters have been constructed for attack detection solutions of botnet attacks. The framework proposed provides hierarchical models to build a monitor and control process to classify the network traffic data to the virtual machine to significantly improve attack detection and mitigate attack consequences. Hence malware hunter achieves the good detection performance against all types of network and host based intrusion evolving.

6. ACKNOWLEDGMENT

I would like to express my deep thankful to Dr.A.V.RAMANI, M.Sc.M.PhIl.Ph.D Head & Guide, Department of Computer Science, Sri Ramakrishna Mission Vidyalaya college of Arts and Science, Coimbatore for his valuable guidance and encouragement throughout the paper and providing necessary facilities to this work.

7. REFERENCES

[1] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker, “Detecting Spam Zombies by Monitoring Outgoing Messages,” IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198-210, Apr. 2012.

[2] NICE: Network Intrusion Detection and Countermeasure selection in Virtual Network Systems, Ritika Saroha and Sunita, International Journal of Computer Science Engineering and Technology(IJCSET) | May 2014 | Vol 4, Issue 5,158-160, ISSN : 2231- 0711

[3] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, “BotHunter: Detecting Malware Infection through IDS-driven Dialog Correlation,” Proc. 16th USENIX Security Symp. (SS ’07), pp. 12:1-12:16, Aug. 2007.

[4] G. Gu, J. Zhang, and W. Lee, “BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic,” Proc. 15th Ann. Network and Distributed Sytem Security Symp. (NDSS ’08), Feb. 2008.

[5] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, “Automated Generation and Analysis of Attack Graphs,” Proc. IEEE Symp. Security and Privacy, pp. 273-284, 2002,

[6] “NuSMV: A New Symbolic Model Checker,” http://afrodite.itc. it:1024/nusmv. Aug. 2012. R. Sadoddin and A. Ghorbani, “Alert Correlation Survey: Framework and Techniques,” Proc. ACM Int’l Conf. Privacy, Security and Trust: Bridge the Gap between PST Technologies and Business Services (PST ’06), pp. 37:1-37:10, 2006.

[7] L. Wang, A. Liu, and S. Jajodia, “Using Attack Graphs for Correlating, Hypothesizing, and Predicting Intrusion Alerts,” Computer Comm., vol. 29, no. 15, pp. 2917-2933, Sept. 2006.

[8] S. Roschke, F. Cheng, and C. Meinel, “A New Alert Correlation Algorithm Based on Attack Graph,” Proc. Fourth Int’l Conf. Computational Intelligence in Security for Information Systems, pp. 58-67, 2011.

[9] M. Frigault and L. Wang, “Measuring Network Security UsingBayesian Network-Based Attack Graphs,” Proc. IEEE 32nd Ann.Int’l Conf. Computer Software and Applications (COMPSAC ’08),pp. 698-703, Aug. 2008.

[10] K. Kwon, S. Ahn, and J. Chung, “Network Security ManagementUsing ARP Spoofing,” Proc. Int’l Conf. Computational Science and ItsApplications (ICCSA ’04), pp. 142-149, 2004.