Journal of Advanced Research in Cloud Computing, Virtualization and Web Applications
Volume 1, Issue 2 - 2018, Pg. No. 1-4
Peer Reviewed Journal

Research Article

An Approach towards Security for Cloud Environment with Regards to Botnet Attack

Ram Kumar Sharma[1], Vijay Kumar[2]

[1,2] Assistant Professor, IIMT College of Management, Greater Noida, U.P.

Abstract

Cloud computing is emerging as a legitimate alternative model for the sourcing and provision of digitized platforms for business organizations today. Cloud provides Platform as a Service (PaaS), Software as a Service (SaaS) an Infrastructure as a Service (IaaS) and promise reduced IT costs and complexity, combined with improved access and flexibility. Botnet is the collections of bots or collection of compromised computers that are remotely controlled by its BotHerder. The term 'Bot' is nothing but a derived term from "ro-Bot" which is a generic term used to describe a script or sets of scripts designed to perform predefined function in automated fashion.

Today's Malware and Botnets are recognized as a global problem and therefore reside in a complex system with many dependencies. Millions of computer systems are infected with often multiple types of malware. These computer systems are organized in several hundreds of different botnets.

Hence the objective of thepaper is to implement or create a secure cloud computing environment against botnet attack.

Keywords: Cloud Computing, Cloud provides Platform as a Service (PaaS)

Introduction

Cloud Computing: Cloud Computing is defined as a computing paradigm where services and data reside in shared resources in scalable data centers, and those services and data are accessible by any authenticated device over the Internet.

Some key attributes that differ the cloud computing from conventional computing are:

- Abstracted and offered as a service.
- Built on a massively scalable infrastructure.
- Easily purchased and billed by consumption.
- Shared and multi-tenant.
- Based on dynamic, elastic, flexibly configurable resources.
- Accessible over the Internet by any device.

Today, we have identified three main categories of cloud services that fall within our broad cloud computing definition.

Software as a service (SaaS): Software deployed as a hosted service and accessed over the Internet world.

Platform as a service (PaaS): Platforms that can be used to deploy applications provided by end customers or partners of the PaaS provider.

Infrastructure as a service (IaaS): Computing infrastructure, such as large servers, storage, and network, delivered as a cloud service, typically through virtualization.

Botnet: Botnet is used to define networks of infected end-hosts, called bots that are under the control of a human operator commonly known as a Botmaster. Hence these following services are provided by bots to its Botmaster:

- Robust network connectivity
- Individual encryption and control traffic dispersion
- Limited Botnet exposure by each Bot
- Easy monitoring and recovery by its Botmaster

Expected Benefits and Risks

My decisions about how and when to move services to clouds are based on the balance between risk and reward.

Corresponding Author: Ram Kumar Sharma, IIMT College of Management, Greater Noida, U.P.
E-mail Id: rushtorams@gmail.com
Orcid Id: https://orcid.org/0000-0002-8841-1730
How to cite this article: Sharma RK, Kumar V. An Approach towards Security for Cloud environment with regards to Botnet Attack. *J Adv Res Cloud Comp Virtu Web Appl* 2018; 1(2): 1-4.

As the technology evolves, I expect this balance to shift so that the benefits begin to outweigh the risks for a growing number of applications and services.

Benefits

Potential benefits of cloud computing includes:

Agility, Adaptability and Flexibility

A business organization that wants to implement a new application can do so relatively quickly using cloud computing services, compared with weeks or months it can take with the traditional enterprise model of buying servers, installing them, and then installing the application to the new servers. In many cases, users can purchase cloud services with a credit card/ debit card and begin to use them almost immediately.

Because cloud computing is built on a massively scalable and shared infrastructure, cloud suppliers can in theory quickly provide the capacity required for very large applications without long lead times. Purchasers of Infrastructure as Service capacity can run applications on a variety of virtual machines (VMs), with flexibility in how the VMs are configured. Some cloud computing providers have developed their own ecosystem of services and service providers that can make the development and deployment of services easier and faster. Adding Software as Service capacity can be as easy as getting an account on a supplier's host.

Cloud computing is also appealing when we need to quickly add computing capacity to handle a temporary surge in requirements. Rather than building additional infrastructure, cloud computing could in principle be used to provide on-demand capacity when needed.

Cost Savings

There is a perception that cloud computing can reduce many type of costs. To date, savings have generally been more clearly shown for small to medium-size businesses. Cost savings can be a big factor in propelling enterprise cloud adoption. The relatively low upfront cost of Infrastructure as Service and Platform as Service, including VMs, storage, and data transmission, can be attractive especially for addressing tactical, transient requirements such as unanticipated workload spikes. An unique advantage is that most businesses pay only for the resources reserved; there is no need for capital expenditure on servers or other hardware.

Risks

A "Risk" is the likelihood of a threat agent taking advantage of vulnerability and the corresponding business impact.

The features that make cloud computing so demanding, combined with the fact that services are accessible publicly, can also lead to many potential risks. ENISA classifies Cloud Computing (CC) risks into three categories:

- Organizational Risks
- Technical Risks
- Legal Risks

Generally Cloud Computing is based on a new utilization of technology and many risks that used to be present in other technological implementations do still exist, and are realized as not cloud specific. Risks like social engineering, physical security, lost or stolen backups, and loss or compromise of security logs are just a few examples of such general security risks.

Hence a list of some tasks needed to secure a cloud system against Malware/ Botnet attack which are:

1. Develop a list of all known Botnets and a data repository for associated traffic data samples that could be used to develop and test detection and mitigation algorithms in future to detect attack.
2. Develop an algorithm using the characteristics which can be identified as common among all Botnets as 1st order detector.
3. Determine if it is practical for all network providers to use network flow data to detect and mitigate Botnets.
4. Go through the several ideas developed and its possible extension to build anti-bot applications that could be applied the way anti-virus or anti-spyware are used today.
5. Development of a robust Botnet capable of maintaining control of its remaining bots even after a substantial portion of the Botnet population has been removed by defenders.
6. Find a way to prevent significant exposure of the network topology when some bots are captured by defenders.
7. Rechecking and finding out the complete information of Botnet by its Botmaster.
8. Create a program that either prevents or warns you about navigating to a known spyware site.

The relevance of ongoing work in certain fields of detection and analysis of security incidents is increased by the advent of cloud computing:

1. Virtual-machine introspection is uniquely suitable for incident analysis in a cloud context; further research about virtual-machine introspection in general and its use for incident and risks handling in the cloud should be conducted.
2. To make the most of virtual-machine introspection and the snapshot feature of virtualization, research in memory forensics must be intensified.
3. The collection of information via live forensics on running systems must be subjected to a systematic approach.

4. Methods for incident detection and analysis based on event information such as log file correlation and visualization must be improved and adapted to the specific requirements on incident handling in the cloud. This is of special importance for incident handling in PaaS and SaaS contexts, where most relevant information will be available as event logs.
5. Detection methods that allow for detection with little or no information about the infrastructure that is monitored (e.g., virtual machines under customer controlas treated by Christodorescu et al. [6] or web applications under customer control as treated by machine learning / anomaly-detection approaches to web-application firewalling) must be improved.

Botnet Attack

A Botnet is a tool for malicious users (attackers). Botnet used for financial gain or for destructive purposes and to misuse or steals the valuable data of users. Hence here some of Botnets attacks are:

- DDoS (Distributed Denial of Service) attacks
- Spamming
- Click fraud/Harvesting of information
- Spreading new malware
- Manipulating online polls
- Google AdSense abuse

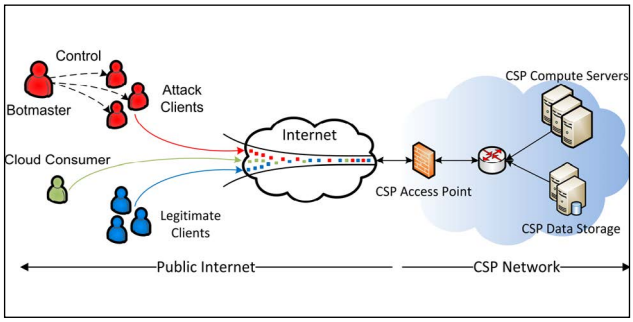

Figure 1.Cloud Network Attack Diagram

How a Botmaster can attack in a cloud environment

Hence among the various type of Botnet attack, attackcan be performed by Botmaster inside a cloud environment as:

Emerging Botnet use in future

1. Malware and Botnets on Mobile Phones
2. Appearance of White Worms
3. More Complex And Potentially Dangerous Malware
4. Advances of Botnet Infrastructure And Distribution
5. Fast Flux Service Network Based Bot

Botnet Detection

Usually Botnet detection and tracking becomes a major research topic in recent years due to increase in the malicious activity. Due to the presence of malicious activity (Botnet) from a long time, very limited formal studies have examined the Botnet problem. So multiple techniques have been proposed to detect Bot which are described as follows:

Honeynet-based methods

Generally Honeynet based method consists of Honeypot and Honeywall.[10] Honeypot denotes an end host which is very vulnerable to malicious attacks and is mostly successfully compromised in a very short time span. And Honeywall denotes software which is used to monitor, collect, control, and modify the traffic through the Honeypot, e.g. Snort. [1, 4] Honeynet work used only unpatched versions of all versions of Windows as Honeypot, and Snort inline used as Honeywall device to track Botnets on a daily basis report (i.e., the Honeynet would have been rebuilt in a day). So based on using both results we identified the location and behavior of bots in a network.

Now beside of this functionality, this paper has also listed a set of suggestions from which we can elaborate “how to write a useful Botnet tracking IRC clients”. [10] First, this client shall have SOCKSv4 and multi-server support to tracking bots. Second, some useful packages, such as lbadns, libcurl, and Perl Compatible Regular Expression (PCRE) shall be included in this client. And at last, the modularity and certain functionalities, such as no threading, shall be inconsideration throughout the design of this client.

A similar Honeynet has been constructed[1, 10], in which Honeywall element shall be able to capture and inspect all the traffic payloads to retrieve Botnet information such as the DNS/IP address of the C&C server with the corresponding port number and the authentically data to join the C&C channel and capable of isolating the Honeypots from other machines in the local network by blocking outgoing connections containing suspicious keywords linked to possible malicious activities. These papers only offer a single vantage point of view on Botnet activities, thus missing a substantial portion of Botnet spreading behaviors.

So in order to capture the comprehensive actions of the Botnets, Rajab et al.[2] have constructed a multifaceted and distributed measurement infrastructure by combining a modified version of the nepenthes platform with the Honeynets i.e. we can say confidentially here, Honeynet is a powerful tool for understanding Botnet technology and characteristics, and tracking Botnet behaviors.

Passive traffic monitoring

Beside of a successfully paperHoneynet, to collect Botnet data or attacker location is a difficult task much more today. So another approach is setting up here “passively monitor the real Internet traffic” which is used to detect or extract the Botnet related packets.[10] Till today, presence of various types of numerous data such as Internet traffic data, DNS data, BGP route views, Netflow data, and proprietary enterprise data, and on the complexity and response time

requirements, many Intrusion Detection System (IDS) designs have been already proposed to detect the Botnets and their location but no solution is perfect to give a better result in compare to this technique. This approach classified as behaviour-based, DNS-based, and data-mining based respectively as described and summarized in the following sections:

This technique classified as:

1. **Behavior based technique:** Based on the presence information and data, this method can be further categorized into two ways

- Signature-based detection
- Anomaly-based detection

2. **DNS-based detection:** This technique is a hybrid of behaviour based and data-mining based approach which is performed on DNS traffic.
3. **Data-mining based detection:** This approach is widely used to detect the Bot in an abnormal traffic and in a high volume of traffic data.

Proposed Integrated Model

Hence in future my researchwork will on cloud integrity and blinding issues in service provider layers.

Proposed Integrated model should include:

- Nebulas
- CloudViews
- Trusted Cloud Computing Platform
- Private Virtual Infrastructure (PVI) and Locator Bot
- Trading storage for computation

Conclusion

Results (Expected): Integrated Proposed Model with reasonable security parameters provide a higher-level security for above issues. And as discussed cloud computing is an emerging area in internet history. So in our proposed method we want to develop a secure system against malware or botnet attack with easy accessible, good reliable and flexible results for its users.

References

1. West Brown M, Stikvoort D, Kossakowski KP et al. Handbook for Computer Security Incident Response Teams (CSIRTs). Technical Report CMU/SEI-2003-HB-002, Carnegie Mellon SEI, 2003.
2. Buyya R, Ranjan R, Rodrigo N. Calheiros Inter Cloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services. Springer LNCS, 2010.
3. Liang-Jie Z, Qun Zhou . CCOA: Cloud Computing Open Architecture. IEEE International Conference on Web Services, 2009.
4. Kandukuri BR, Ramakrishna Paturi V, Atanu Rakshit. Cloud Security Issues. IEEE International Conference on Services Computing,2009.
5. George Resse. Cloud Application Architecture. OReilly, 2009.
6. Buyya R, Yeo CS, Venugopal S. Market-Oriented Cloud Computing:Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. HPCC, 2008.
7. Reddy VK, Reddy LSS. Security Architecture of Cloud Computing. *International Journal of Engineering Science and Technology (IJEST)* 2011.
8. Kamal Dahbur et al. A Survey of Risks, Threats and Vulnerabilitiesin Cloud Computing, ACM, 2011.
9. Bernd Grobauer et al. Towards Incident Handling in the Cloud: Challenges and Approaches, ACM, 2010.
10. Tyagi AK, Aghila G. A wide survey on botnet, IJCA,November 2011.

Date of Submission: 2018-12-10
Date of Acceptance: 2018-12-18