A Study on Botnet Detection in Cloud Network

Parneet Kaur
Research Scholar, Department of CSE, CGC College of Engineering, Punjab
Email Id: Pkneetu45@gmail.com

Dr. Anuj Gupta
Professor, Department of CSE, CGC College of Engineering, Punjab
Email Id: er.anujkgupta@yahoo.com

Abstract. Cloud computing is a infrastricure that enable business oppurnities to the companies to put the resources over the internet and provide access to the end users based on "use as pay basis" model. The modern business is already in the stage of shifting on the cloud to take the technology benefit of the cloud resources. The technology is maturing now and many cloud service providers are giving the services to the scalable infrastructure by enabling "pay as you go model" that fullfill the computing need and requirements of the end user & business companies. The focus of the cloud security reseacrh is the protection of end user who are using the cloud services connected over the internet from the attacks that use any propagation models such as external, insider and malicious users. Cloud infrastructure is established and enabling the technological benefits to the usres, however little attention is given to the cloud security to defend against the attackers to launch attacks using the cloud services, For example, if user is accessing the cloud services as an VM Instance and malicous user may take the control by hijacking the session between the end user and cloud infrastructure.

This paper discuss the Botnet threats in cloud based infrastructure and a review on current detection techniques put in place to defend against such threats. The Botnet is major threats in internet eco-system that include cloud based sevices, IoTs, Deep Networks. The end users connected to the internet or cloud based services are more prone to botnet threats as they are less tech-savy persons. The state-of-art models for botnet detection in cloud enviornment is presented in this paper. In the end, an architectural view of a models of botnet threat detection based on the outbound DNS traffic monitoring is presented that incorporate the novel light weight honeypot application in the cloud infrastructure.

Keywords: Cloud Computing, Botnets, DDoS, Malwares, Cloud Security, IoT

1 Introduction

Over the years botnet is becoming the biggest threat to the internet eco-system across the globe. However botnet threats is not a new one, history starts at least from 1999 when two heart breaking attacks- the Pretty Park[1] work and the Sub7 Trojan[2] which demonstrated in real way how infected computers had received the commands by listening on the IRC[3] chat applications.

Botnet evolution: from IRC nuisance to Cyber Crime Infrastructure:

In the early days, IRC was one of the majorly used mechanisms for distribution of command instructions to bot infected resources, like the one used in GTbot botnet threats in year 2000 that took advantage of popular mIRC chat applications e.g. a Microsoft Windows Applications. Further back to history in the year 1995, the scripting language was being used by the attacker so that they could pull off more sophisticated schemes, including distributed denial-of-service attacks [4].

In current internet eco-system, the botnet are best used by the attacker as tool to steal the financial information, performing DDoS attacks, click frauds, and gaining the full assets of the organizations.

It is not possible to present every details of modern botnet, but most common characteristics of them can be highlighted as:

- Different Command and control architectures: Centralized architecture in case of IRC and HTTP protocols whereas modern botnets is also adopting P2P as decentralized model as well as more random architectures has been used by them in recent times.
- Attack surface has been shifted from well known DDoS attacks to steal informations, spam and even targeting critical infrastructures such as SCADS, Power Grid, Financials sectors etc.
- Historically botnet has evolved from IRC then HTTP protocols and in a current scenario a P2P model is adopted.
- More effective evasion mechanisms has been started to use by botnet creators such more powerful

encryptions, compressed communications, fast Flux domain's communications etc.

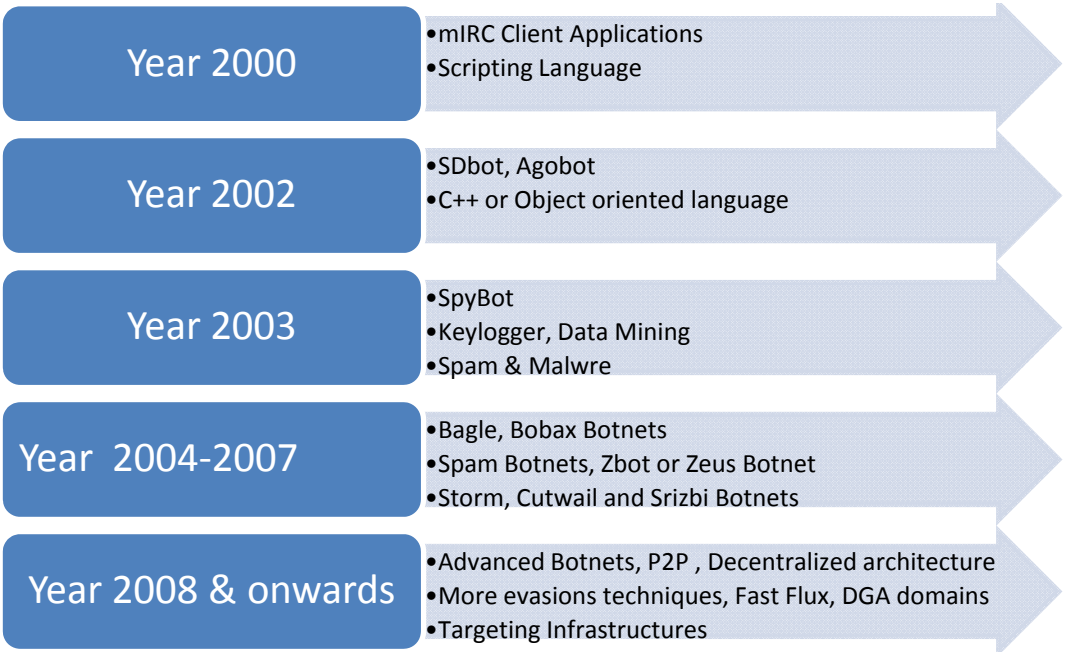

Figure 1: Evolution of botnets during 1999-2007

2. Botnet Infection Life Cycle

Figure 2 depicts the typical botnet infection life cycle. Whenever the botmaster want to infect a system, he has to go through the proper procedure to perform it in well formed steps:

1. Initial infection
2. Secondary injection
3. Connection creation
4. Sending the malicious code
5. Maintenance & Update

Firstly, a botnet infect a new vulnerable system that is prone to be infected and weak point that is easily compromised. Then the botnet inject some malicious code into victim machine using different protocols such as HTTP, FTP, and P2P etc. After successfully injecting the malicious code, the victim device automatically make a connection with already existing command and control server. Once a malicious code is injected to the victim device then it becomes a zombie. In the fourth step the botmaster send commands the bot army through the command and control server [5-6]. The malicious activities will be performed as per the instructions received in the command from the C & C server [7]. Finally the task is to maintain and update the zombie active all the time, it send updates to the zombie devices time to time[8][9].

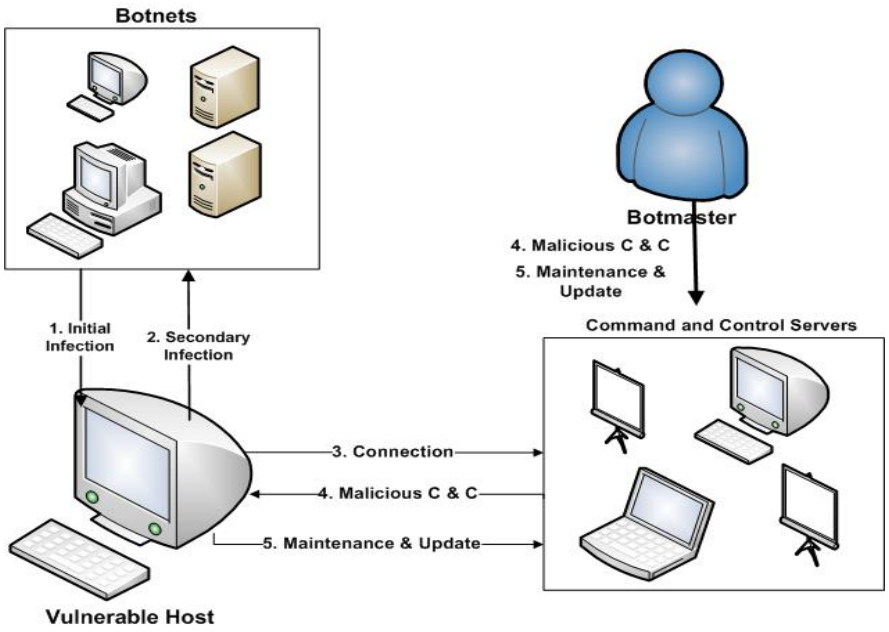

Figure 2: Typical steps in Botnets

3. Botnet Deection Mechanims in Cloud Networks

Botnet is a major problem for internet eco-system which is remotely controlled and managed the botmaster. The botnet attacks are different than the normal class of attacks as they are not easy to tackle and there multiple entities involved into it such as Botmaster, Command and control server, infected resources etc. According to the published research in multiple publishing bodies such as ACM, Springer, IEEE etc, the detection mechanism implemented to defend against the botnets can be categorized broadly into two main categories which can be later divided into multiple sub-categories [10-12] as depicted in figure 2:

- Honeynets detection techniques
  - Low interaction Honeypots
  - High Interaction Honeypots
- Intrusion detection techniques
  - Signature based detection
  - Anomaly based detection

Honeynets & Honeypots Based Detection System:

To detect the cyber attacks, the end user system are the best way to collect the evidences as the attacker directly target the end user system because they are more prone to be infected by the attacker. The Honeypots or Honeynets represent these resources in the form of vulnerable system which are designed to be attacked the attacker. The value given by Honeypot/Honeynets is very rich with low false rate and can be treated as Indicator of Compromise performed by the attacker. The attack logs can further analyzed to know the actual source and level of infections. As per the various research conducted, botnet has started to change signatures time to time and thereby making the detection of signature based approach a challenge to detect them [13-14]. In this case the Honeynets/Honeypots are powerful mechanism to capture, collect and log the attacker activities.

IDS (Intrusion Detection System):

Intrusion detection system mainly monitor the network traffic of a network and if there are some deviation of normal behavior of traffic noticed in that network, the alerts can be raised to detect it. During the analysis, the deep packet inspection algorithm and net flow based analysis can be performed to confirm the attack in a network. IDS have capabilities to block the traffic corresponding to the malicious activities of a virus or malware spreading in a network. Intrusion detection system can be broadly classified into A) Signature based detection B) Anomaly Based detection

A) *Signature Based Detection:* In this botnet detection approach, the malware are treated as known set of sequences followed and spreading a network. Based on these certain set of rule, this technique will be able to detect the known class of attacks in a network, The strength of this approach is purely depend on the signature database associated with them [15-16].

B) *Anomaly Based Detection:* In this technique, the criterion of normal behavior of a network is defined, if anything found anomalous that can be feed as input to the network manager to look upon [17]. The normal

activities of a network are configured by the network administrator on a edge device of a network. For example access control list based Rate-limit define the threshold placed on an IP address in that network, If that particular IP address generating the traffic beyond that threshold then it can be treated as alarm to further dig out any probable infection in that particular PC. These types of detection system are based on statistical analysis model or traffic behavior analysis based which detect those events not related to the normal model of a network. The problem with such detection method is that they are bit expensive with respect to the computation involved but they are more secure than signature based detection comparatively.

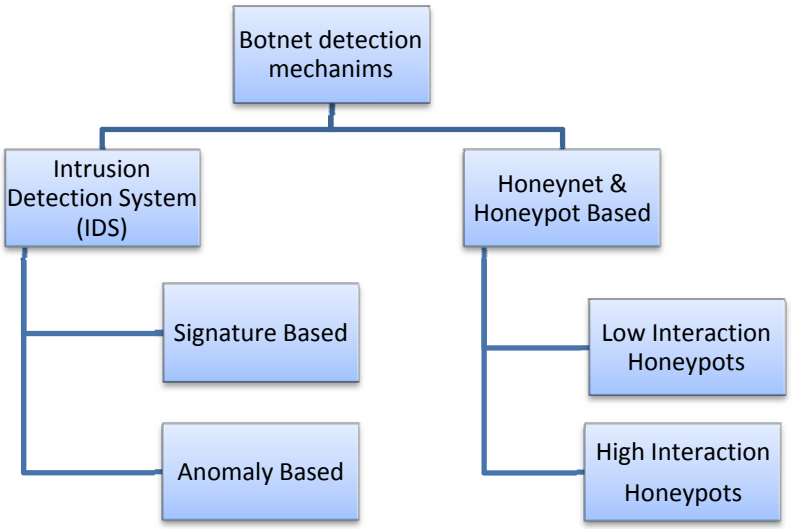

Figure 3: Botnet Detection Mechanims

4. PROPOSED FRAMEWORK FOR BOTNET DETECTION IN CLOUD ECOSYSTEM

Based on the research study and state of art botnet detection mechanims, here the botnet detection framwork in cloud network is presented as shown in figure 4. The VM resource assigned to the end user are being monitored by desinging and implemening the light weight honeypot applications installed over it. The outboud communcations of the VM machine will be logged and later analysed to determine the botnet infections in cloud netowk. The prototype design of proposed model is depicted in figure 3.

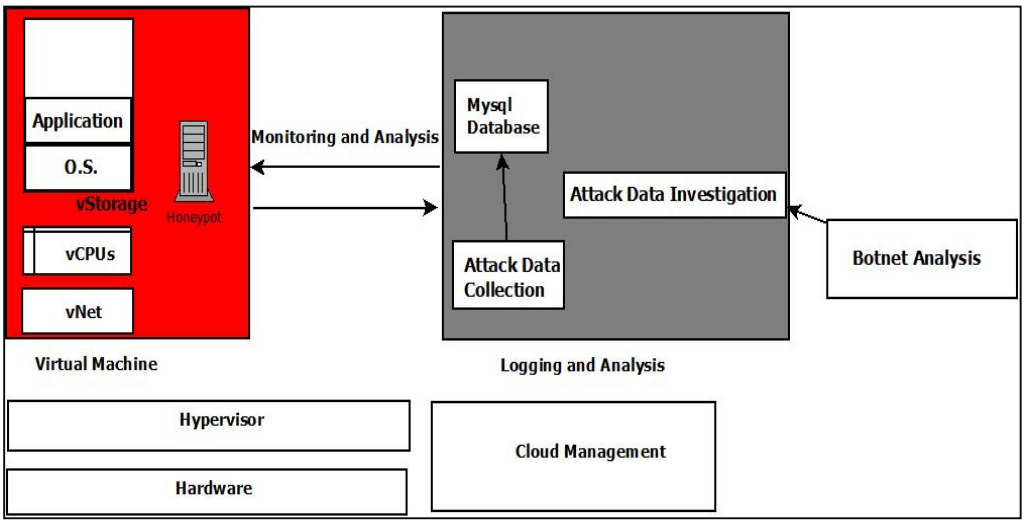

Figure 4: Proposed System Design

Conclusion and future work:

Cloud computing is providing the business opportunities to the companies and users can directly access the resource hosted somewhere on the internet by merely having a PC and internet connectivity. In current internet world, everybody is directly or indirectly connected to it and our day-to-day life is affected by it. The companies start to shift their business resources over the cloud and end user is directly accessing them by subscribing or paying against those resources. In this paper the botnet threats targeting the internet eco-system and is becoming more powerful and dangerous to the resources is presented. The detection methods of botnets are presented and it is highlighted that by only applying a single detection mechanism it is quite impossible to

defend against them. So there is a need to apply different techniques and need to apply subject knowledge of data mining, DNS traffic analysis, Artificial Intelligence to detect and defend against them in real time scenario. In the end the prototype design of Botnet detection is cloud network is presented that integrate the novel approach of the outbound DNS traffic monitoring of VM Honeypots as cloud resource.

References:

[1] virus.wikia.com/wiki/Prettypark
[2] https://en.wikipedia.org/wiki/Sub7
[3] https://www.mirc.com/
[4] blog.trendmicro.com/the-state-of-botnets-in-late-2015-and-early-2016/
[5] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, "Botnets: A survey," Comput. Networks, vol. 57, no. 2, pp. 378–403, Feb. 2013.
[6] M. Feily, A. Shahrestani, and S. Ramadass, "A Survey of Botnet and Botnet Detection," 2009 Third Int. Conf. Emerg. Secur. Information, Syst. Technol., pp. 268–273, 2009.
[7] I. Lin and C. Peng, "A Survey of Botnet Architecture and Batnet Detection Techniques," vol. 0, no. 0, pp. 81–89, 2014.
[8] N. Hachem, Y. Ben Mustapha, G. G. Granadillo, and H. Debar, "Botnets: Lifecycle and Taxonomy," 2011 Conf. Netw. Inf. Syst. Secur., pp. 1–8, May 2011.
[9] J. Govil, J. Govil, C. Science, and A. Arbor, "Criminology of BotNets and their Detection and Defense Methods," pp. 215–220, 2007.
[10] X. Zang, A. Tangpong, G. Kesidis, and D. J. Miller, "Botnet Detection Through Fine Flow Classification," no. 0915552, pp. 1–17, 2011.
[11] H. S. Nair and V. E. S. E, "A Study on Botnet Detection Techniques," vol. 2, no. 4, pp. 2–4, 2012.
[12] A. Sgbau, "A Review-Botnet Detection and Suppression in Clouds," vol. 3, no. 12, pp. 1–7, 2013.
[13] M. Abu Rajab et.al: "A multifaceted approach to understanding the botnet phenomenon," ACM SIGCOMM, 2006.
[14] T. H. Files, "Botnets: Big and Bigger," pp. 87–90, 2003.
[15] D. S. Eth-tutor, B. T. Supervisor, and B. Plattner, "Signature-based Extrusion Detection," no. August, 2008.
[16] K. M. C. Tan et.al: "Undermining an Anomaly-Based Intrusion Detection System Using Common Exploits," pp. 54–73, 2002.
[17] C. Liu, C. Peng, and I. Lin, "A Survey of Botnet Architecture and Batnet Detection Techniques,".