International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-3 Issue-5, November 2014

Zombie Attack: Need of Advance Prevention

Laxmi Shankar Awasthi, Himanshu Pathak, Parth Singhal

Abstract*: Cloud security remains very popular these days, Since Industries are moving towards cloud services very rapidly. Security of cloud from data theft and data monitoring is still be debated. There are various ongoing research on how data can be secured and safe from the intrusion. But it is the matter of concern that there are no headway available for the permanent security against the zombie. Zombie attack is advancing day by day and it is difficult to detect in a network In this paper Author present an approach to explain the importance that up to what extent the zombie attack can be vulnerable for the society.

***Index Terms*: Zombie, botnets, DDoS**

I. INTRODUCTION

Cloud is providing interesting features like on demand services, pay as per your services. Services can be serve to both public cloud and private cloud. Cloud computing originates from distributed computing, it is a collaboration of different technologies. Like other networks, cloud computing also has its security issues. One of the most popular threat is plotting a zombie in a network. Many data fraud and Trojan attacks can be achieved through this attack. According their advancing technology it is very popular amongst hacker. Zombie is a computer i.e. connected to a network and controlled by the hacker. Many a time user is unaware of its infected computer. This can infect autonomous computer or a network through DDoS and Botnet attack can be done by a zombie computer also.

Zombie is also known as Bot computer that is controlled by the hacker and setup for the forward transmission. This forwarding capability of an autonomous systems in a network will result to the origin of zombie army (Botnet). Through zombie army, particular web server or site can be attacked by doing ping operations or forwarding the spam by botnet. There are many ongoing research available but detection mechanism artificial immune system **[1]**. This might help in reducing the risk of zombie in cloud. In this paper we will discuss the amount of security breaches by a zombie, and how this affect the network in a cloud.

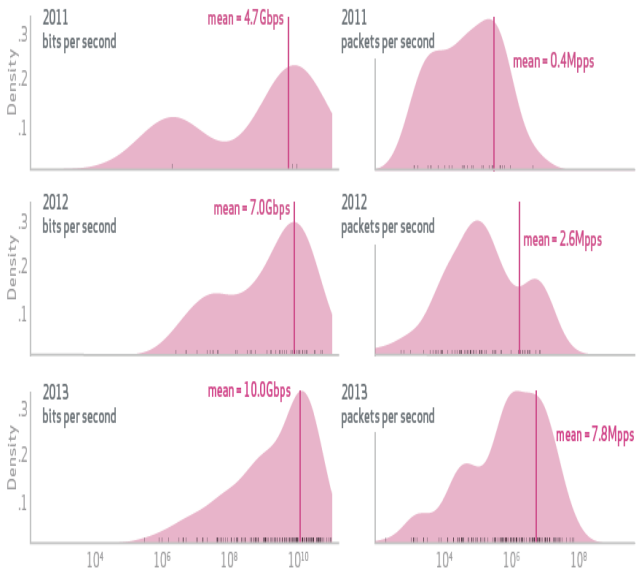
This paper is divided in to 4 sections viz.

1. Introduction
2. DDoS attack over cloud
3. Botnet attack
4. Conclusion

Revised Manuscript Received on 30 November 2014.
* Correspondence Author
Dr. Laxmi Shankar Awasthi*, Department of Computer Science, Lucknow Public College of Professional Studies, Lucknow (U.P.), India.
Himanshu Pathak, AIIT, Amity University, Lucknow (U.P.) India.
Parth Singhal St. Francis College, Lucknow (U.P.) India

II. DDOS ATTACK

DDoS attack is used to make web server unavailable to its user .It is done by the multiple compromised system in a network .Users are unaware of their compromised system and were remotely controlled by the hacker. DDoS attacks majorly targeted on Internet Data centers, online gaming ecommerce, E- Financial services .Its functionality is to reduce the bandwidth by exploiting the server and degrade the user experience. There are various DDoS zombie tools available to exploit the server like Zombie puppet, Storm, Madman etc. But among all LOIC is very popular, the hacker used this tools to attack Facebook on January 28, 2012 **[2]**. DDoS attack can also be defeated by employing the idle resource of the cloud to clone sufficient intrusion prevention servers **[3][4]**



. Figure1: Denial of Service attack bandwidth and packet count levels 2011-2013 [5]

According to the report of Verizon data breach investigation report from the year 2011-2013 security breach continuously increases.

III. BOTNET ATTACK

Botnet scan the list of IP addresses in a network and check vulnerabilities on which attack can be easily made without tracing back the operator. It is also estimated that botnets are also used to send spam and malware, 97% of E-Mail we received is not required. And majority of spam is generated by using botnet **[6]**. To minimize the risk of this attack we have to update the patch of operating system and install a proper gateway defense solution **[7]**. Intrusion detection system is also introduced to monitor host and analyze the traffic to handle Botnet attacks.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

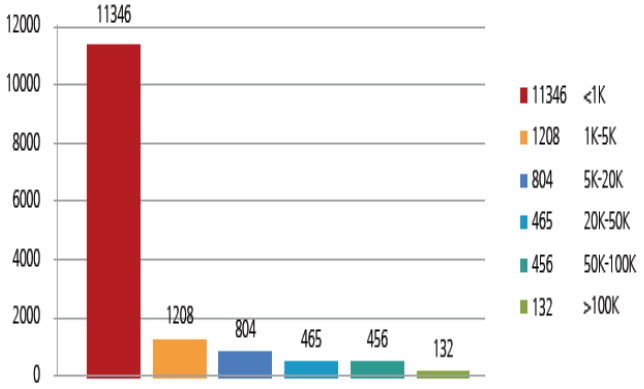


Figure 2: Botnet Distribution

"According to Huawei cloud security center statistics, the global distribution of botnet hosts in China and the U.S. are 30.3% and 28.2%, respectively, much higher than that of other countries. Most botnet controllers are located in the U.S., occupying 42.2% of the total number and followed by Germany (9.1%), France (7%), Britain (5.8%), and China (3.8%)." **[2]**

IV CONCLUSION

Various researches are published to prevent from zombie attack. The key concept behind most of the researches is to monitor outgoing messages is .This can be done by SPOT (Sequential Probability Ratio Test) **[8]** .This is an automated system which helps to find the compromised machines in a network. Advancing zombie attack should be taken into granted, so that the risk factors by the compromised system should be decreased. BotSniffer is also used to detect and minimize the risk of zombie attack. However if we compare to the advancements of zombie attack and the emerging technology used to minimize the risk. It is still can be debated that machine in a network is secure or not?

REFERENCES

1. IEEE April 29 2014-May 1 2014, A cognitive approach for botnet detection using Artificial Immune System in the cloud by Kebande, Victor R. ; Information and Computer Security Architecture(ICSA), Research Group, Department of Computer Science, University of Pretoria, Lynwood Road, Private Bag X20, Hatfield 0028, Pretoria, South Africa ; Venter, Hein.S. In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2014 Third International Conference .
2. 2013 Botnets and DDoS Attacks Report by Huawei Enterprise ICT solutions a better way..
3. IEEE Parallel and Distributed Systems, IEEE Transactions on (Volume: 25, Issue: 9), Sep 2014, Can We Beat DDoS Attacks in Clouds? By Shui Yu ; Sch. of IT, Deakin Univ., Geelong, VIC, Australia ; Yonghong Tian ; Song Guo ; Wu, D.O..
4. Cloud Computing: Analyzing Security Issues & Need of Prevention against Vulnerabilities, by Laxmi Shankar Awasthi, Himanshu Pathak, Parth Singhal , International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4, Issue-1, March 2014
5. 2014 Data Breach investigations report, Verizon.
6. Anselmi, D., Boscovich, R., et al. (2010). Security intelligence report. Technical Report Volume 9, Microsoft.
7. A Sorphus Whitepper November 2013, Botnets: The dark side of cloud computing By Angelo Comazzetto, Senior Product Manager.
8. Detecting Spam zombies by monitoring outgoing messages by Peng Chen, Florida State University, 10-17-2008.

AUTHOR PROFILE

Dr. Laxmi Shankar Awasthi is working as H.O.D in Lucknow Public College of Professional Studies in Computer Department. He has published Research papers in various national and International Journals.

Mr. Himanshu Pathak is pursuing M.C.A from Amity University Lucknow Campus in Amity Institute of Information Technology. He has published Research papers in various International Journals.

Mr. Parth Singhal is a student of St. Francis College Lucknow .He will strive to write more research papers on Cloud Computing.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)