Botnet and Botnet Detection Techniques

Rimsha Malik
School of Engineering Science and Technology (SEST)
Jamia Hamdard, New Delhi, India

Bhavya Alankar, PhD
School of Engineering Science and Technology (SEST)
Jamia Hamdard, New Delhi, India

ABSTRACT

The biggest danger to the world of cyber from the past twenty years is botnet which is also responsible for the cases of cyber-crimes lately. A botnet is the network of destructive computers or devices which are managed by the botmaster and the victims are not aware of it. The botnets are generally used by spammers for stealing of data from users of internet worldwide. This paper is an analysis about the existences of the botnet and its management .The world has not got sufficient data and a convincing procedure for detecting a botnet. The hazard of Botnet is not strange to anyone as they are existing from a long time, there is a lot of research that need to be done to put a check on them. Nowadays the things are adding on to check the botnet in the server.A lot of research work has been done on botnet detection ways. However researchers haveadvised ways that are distant from each other on botnets.

Keywords

Bot agents, honeynets, botmaster, threat, command and control server (C&C)

1. INTRODUCTION

All the businesses and services are dependent on the internet and the servers that store the data in the cloud and provide easy access across the globe. It gives several services that are extremely helpful to use. The Internet may be helpful positively but the cyber crimes are prevailing across it as well. The confidentiality and integrity of the data can be harmed by doing breaches in the information security, theft of identity and several other attacks. The person who attacks also known as Botmaster spread Trojan or Malwares or both which increases the bots number present in the network. Bot in the botnet is referred to robot and net to the Internet which states that botnet is a robot network or computer/servers where attacker controls and gains the access of the systems of the network while the end is not even known to it. The bots are used remotely through command and controlling server which is controlled by the Attacker. The attacker usesone of the bots of the botnet which is the command and control server to control and communicate with the other bots through instructions. The bots can be singularly as well as in a group at the same time through commands. Botnet's size can be increased compromising the devices or servers in the network. Botnet sustains the property of propagation which helps it in spreading all over the internet [1]. The attacks that can be done through botnets are the fraud of phishing, fraud of clicks, stealing of password, spamming, fraud of bitcoin, theft of mass identity, traffic sniffing, new malware spreading and logging of the key.

Internet Relay Chat (IRC) and Hypertext Transport Protocol (HTTP) are the communication protocols for botnets [1]. The widely used botnets protocol is IRC as they are extremely popular and it can be easily found for use by a botmaster.IRC server are easily found and taken down if the botnet is detected, which makes a disadvantage of IRC. A zombie computer is a name given to the compromised systems, hence botnet is also known as a zombie network. The most crucial time in the making of the botnet was the first five years. The first botnet created by the attackers which was called as “Eggdrop” in 1993. More advanced botnets are created after that which have new features and functions until 2002. During these years the use of botnets was started bymost of the attackers which resulted in a rapid increase of cyber attacks.

The world has not got sufficient data and a convincing procedure for detecting a botnet. The Hazard of Botnet is not strange to anyone as they are existing from a long time, there is a lot of research that need to be done to put a check on them[1]. Nowadays the things are adding on to check the botnet in the server. A lot of research work has been done on botnet detecting ways. However researchers have advised ways that are distant from each other on botnets. It has been examined that to notice and audit botnets two major ways are used [3, 6]. The major first way is using honeynets by installing them into the servers. This honeynet will isset up to focus on collecting reports of botnets and know the ways they behave. They may not be able to find botnet but it collecting the information which is further used to create a protection for botnets[7].A setup with intentional vulnerabilities is known as honeynet.It main motive is to

get attacked by the botnets,this enables us to study the activities of the attacker and several methods can be developed to secure the network. The second approach for botnet detection is established on quietly checking the network Movement and analyzing it. The approaches which follow the ways for detecting a botnet are the Anomaly based and DNS based detection techniques which has been studied further in the paper. The movement of the DNS server and IDS server is been tracked and any abrupt behavior is saved in to further study the attacker and develop methods to secure the network. This approach is more efficient as compared to other approaches.

2. RELATED WORK

A lot of research has been done in botnet detection. It focuses on different techniques of botnet detection and botnet suppression in this section. H. B.Jethva [1] Haritha S. Nair, Vinodh Ewards [2], Jignesh Vania, Arvind Meniya, gave the mechanism of various botnet detection techniques. A study also gave network-based botnet detection techniques in which network traffic is inspected related to IRC protocol which may sense the presence of a botnet. The method of detection of a botnet which related to alarms when an intruder from a different network.

IRC botnets deployment is done all around in past years. The use of IRC protocol as a C&C method spread because of its versatility, redundancy, and scalability. There are a Large knowledge and code base for IRC-based bots, which enables botnet creators to reuse the source code and create a new botnet, for example, Agobot variants. A well designed and modular Agobot's code is online available, which makes it easy to create their own botnet for botnet author.

The fundamental weaknesses of an IRC botnet is that is stem from its C&C servers which are centralized. The source of command is easily identified and a single point is possessed by these servers, which make it very easy to disrupt a botnet which is based on IRC and get the IP addresses of bots present in a botnet. Botnets which use IRC as communication means for C&C are easy to detect relatively to others. The hostility is adapted by the botmasters towards IRC bots by somehow optimizing the IRC botnet's C&C architecture or by creating a new botnet.

The shift currently is to de-centralized P2P C&C architectures from centralized client-server. The IRC based bots are being changed by the authors to make them resilient because of which IRC bots are still seeing widespread use.P2P botnets are documented and discovered in the wild e.g. Phatbot, Peacomm, Sinit, Slapper and Nugache.The shift is already made to a new botnet C&C control methodology, i.e. P2P .C&C.Following are the approaches which follow the ways for detecting a botnet

1. Detection based on Signature

For detecting a botnets this approach tries to find a signature. It gives us the important instruction around the form of botnet intrusion and it is easy to apply. This approach detects the botnet at very huge percent and most of the detection detected by this are real. No new botnet can be detected by this approach as it has signature saved for only already familiar botnet which can be the only defect in this approach.The correlation produces signature for IDS system.The strategy driven by IDS to detect botnet has problem.The signature produced by the IDS system sometimes cause problem in detection as they can be in encrypted form and it can be difficult to decrypt the signature.The Signature or sign provided by a botnet after detection is saved into the database on this technique,the resistance is created for that particular botnet which is the main drawback as it related to a particular botnet only.If another botnet of same type attacks the system again then it is not able to detect it as it have signature saved of only one botnet of that type,the botnet can attack again and again and this system will not be able to detect the botnet.

2. Detection based on Anomaly

The botnet are detected in this approach by movement irregularity, also known as anomaly on the net[6]. This approach works by analyzing the whole grid and finds each irregular act of the movement all over the grid. The defect in detection based on signs is also removed by this approach as it has the ability to find botnets that are never used in any intrusion. It costs more as compared to detection based on Signature and also superior to it in detecting a botnet. The main two proposed anomaly detection methods are based on resulting large deviations for packet level and flow data. Anomaly represents a set of records of interaction in both type of anomaly detection method.

3. Detection based on Domain Name system

The approach is based on DNS, where botnet is detected by getting the data of the DNS and checking if a botnet connects to the DNS or not which is not like above mentioned approaches. Detection based DNS and anomaly are similar as procedure practiced in detection through anomaly is practiced in DNS movement too. The group of host which behave abruptly are taken into account by this method which are like botnets.DNS TTL is not honored in these group of hosts, DNS queries are carried out to servers which are not local. This methods looks into large number of response from DNS with NXDOMAIN as code of error. This technique is able to detect botnet with high efficiency.

3. METHODOLOGY

The botnet life cycle is a procedure for adding a new bot in a botnet. The different phases for making a botnet or creating a new bot in a botnet is contained in a life cycle. There are different researchers which state differently about the life cycle of botnet. The distinct steps in a lifecycle of botnet are infection and injection, control and command and application of botnet [1,2]. Figure 1 describes about a botnet life cycle.

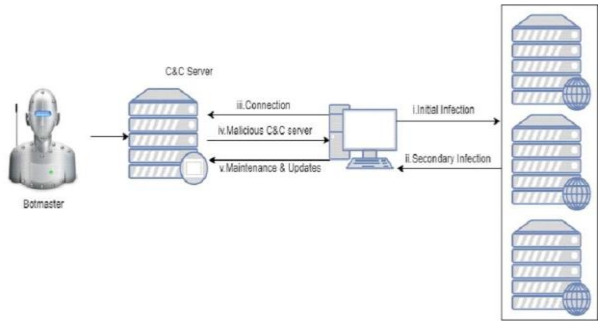

Figure 1: Life Cycle of a Botnet

Other researchers state that the life cycle of the botnet is in five phases: Infecting the server, Injecting to the server, connecting to the server, sends virus to the server and maintaining and updating the botnet [3]. While the botnet infection is inserted into a new device, which is connected to the internet, then the injection of virus in to device by HTTP protocol and P2P protocol which connects to the C&C server of botnet? It starts working as a zombie computer for botnet after malicious code injection into the system. Now the new victim device is controlled by the attacker through command and control server. The masters keep the updating and maintenance work [1, 4].

A. Network Topologies in Botnets

When talking about botnets network topologies needed to be discussed because it creates a huge difference in botnet performing its functions. Different topologies and architecture have been used by attackers [5]. The main topologies botnets uses are:

1) Star Topology

A very good bot managing and communicating system is provided between the bots by this topology. The big disadvantage of this topology is that it have only C&C server, which creates the problem of failing at one place i.e. the whole system breaks if C&C gets blocked. The connection from botnet can be blocked by even a legitimate user themselves [5]. The Main C&C contains all the information that is needed to run the botnet. If the main C&C fails then the botnet is of no harm. One does not need to remove that if the main C&C is not working for a botnet in Star topology. A number of systems that are connected to this type of topology may vary, it can be as few as one or can be in large numbers as hundreds. The risk of connecting several systems to this botnet is high as it become dead if the main C&C server breaks.

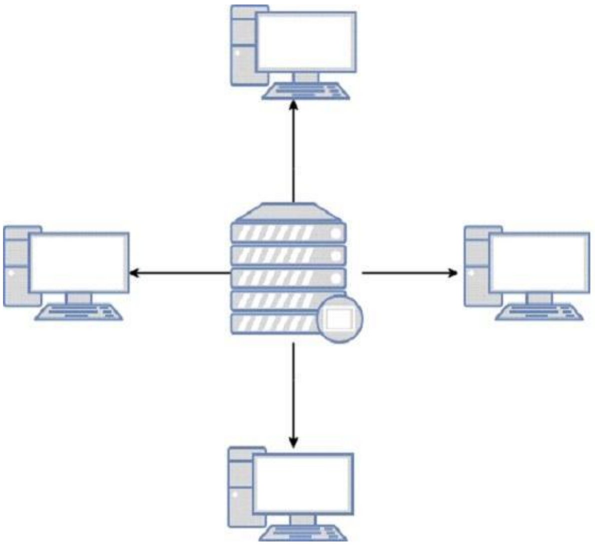

Fig 2 Star Topology

2) *Multi-server Topology*

In this topology multiple servers or C&C controls and manages the network as a whole which makes the communication system better between all C&Cs and bots in the network. For some reasons, if a C&C fail, all other servers remain working and also make a decision about removing the C&C which has failed. The risk failing of the network at a point is removed in this topology[5].This topology is highly efficient as compared to the star topology.The C&C servers in this topology can be many which can create a big network as each C&C server can connect to several other systems.If the C&C server which has many systems connected to it fails then it is replace by other C&C server which also connects to the other systems which were previously connected to the failed C&C server and the operation continues without smoothly. Fig. 2 describes above topology.

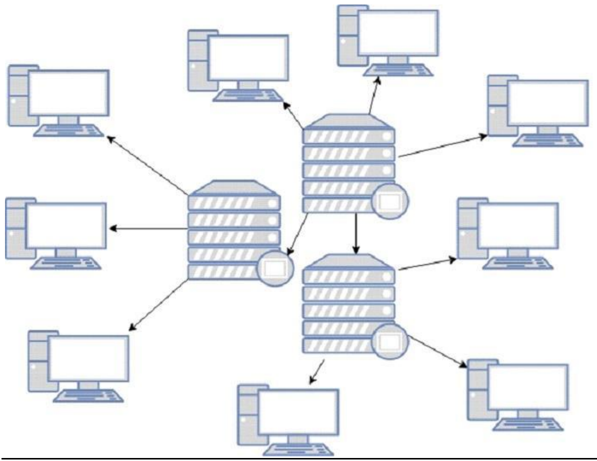

Fig.3 Multi Server Topology

3) *Hierarchical Topology*

In this topology botnet contains multiple C&C servers are set in a way in cluster for providing a reliable network. It is easier for a botmaster in renting a bot due to hierarchical topology. Using hierarchical topology botnets has many benefits as they are not easily detectable. In botnets based on hierarchical topology, the location of the bot agent is not known to the other bot agent which makes it tough to find a botnet and it also does not reveal the botnet size[5]. The botnets using Hierarchical topology is very hard to detect as the C&C servers location is not known if one C&C server gets caught then another C&C server cannot be detected.Each server has many systems connected to it in a hierarchical way so that each level contains a C&C server and make the work faster and easier.The same C&C server can be rented out to many clients and one server can be used to carry out functions for different clients at the same time.It reduces the number of machines used in the botnet which makes it more efficient than the Star topology and Multi server topology.The cost factor also rises in this type of topology as the server increase so it takes space to put data of several clients into a C&C server and use it according to the functions and commands.Hierarchical topology can be very useful and efficient as its servers are distributed all over the network at different levels which reduces the risk of failure in the system.

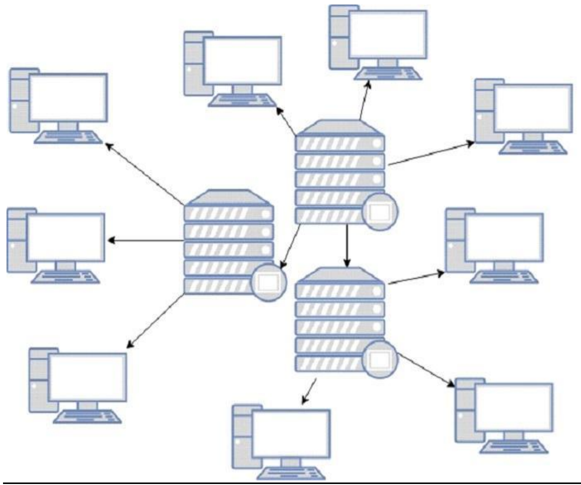

Fig. 4 Hierarchical Topology

4) *Random Topology*

Botnets agents spread the malware through the same procedures although this topology does not contain any centralizes C&C infrastructure. As per the condition any zombie computer can act as a C & C server. Bots can communicate through many paths and ways and in this topology, botnet are very difficult to detect and control as C&C infrastructure is not centralized i.e. a new C&C server will be replaced into the network if a working C&C server is hijacked and is removed by new server. Bots respond to the command given by C&C in more time as compared to other topologies. It is still better to use as it provides many better functions and features than other topologies of botnet [5]. This can also be known as Dynamic master slave or peer to peer relationship topology. In the Dynamic master slave, master refers to the C&C servers while the slave is the system which is dynamic means the master slave keeps on changing.Any system can be a master or a slave at a particular instance of time. The peer to peer relationship is that the system and serve both are treated as peers which can be related to each other in the same way at any given time. The peer remains same as it can act as server and the system as well.

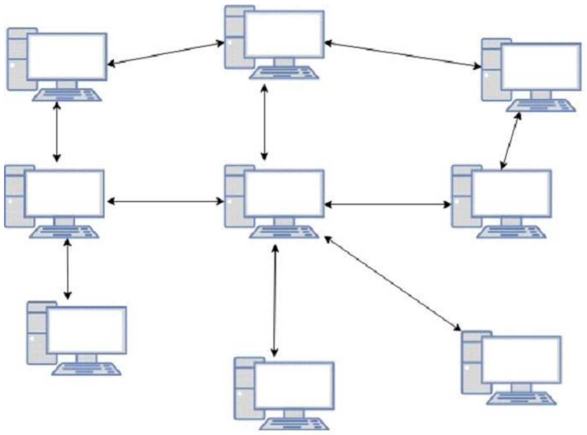

Fig. 5 Random Topology

4. CONCLUSION AND FUTURE SCOPE

In this paper it has analyzed that what are the botnets and what threats they can cause to us . This has been discussed some techniques through which the botnets can be detected and monitored and the network topologies used by the botnets in attacking a server.In the end it states that the internet has become a basic need to everyone around the world nowadays and there are several works running across it.The Cyber thieves uses new techniques everytime to intrude and steal the data through botnets.There is need to create new techniques to detect and remove the botnet from the server without affecting our data and to safeguard our server. Millions of users use the Internet globally as it is becoming more common in the upcoming days. New threats are coming on internet to for attacking users. Botnets are into internet for quite a long time, still emergence is not seen for best detection techniques. A technique is needed to detect and kill the botnet in the network.

5. REFERENCES

[1] S. Anwar, J.M. Zain, M.F. Zolkipli and Z. Inayat, “A Review paper on Botnet and Botnet Detection Techniques in Cloud Computing,” 2014.

[2] N. Hackem, Y.B. Mustapha, G. Granadillo and H. Derbar, “Botnets: Lifecycle and Taxanomy”, 2011.

[3] M. Feily, A. Shahrestani, and S. Ramadass, “A Survey of Botnet and Botnet Detection,” *Third Int. Conf. Emerg. Secur. Information, Syst. Technol.*, 2009.

[4] B. Saha and A, Gairola, “Botnet: An overview,” CERT-In White PaperCIWP-2005-05, 2005.

[5] Gunter Ollmann, “Botnet Communication Topologies,” Damballa Inc.,2010.

[6] Z. Zhu, G. Lu, Y. Chen, Z. J. Fu, P.Roberts, K. Han, "Botnet Research Survey," in Proc. 32nd Annual IEEE International Conference on Computer Software and Applications (COMPSAC '08), 2008.

[7] J. R Binkley and S. Singh. “An algorithm for anomaly based Botnet detection”. In proceedings of USENIXSRUTI’06, pages 43-48, July 2006.

[8] M. Bailey, E. Cooke, F. Jahanian, Y. Xu, and A. Arbor, “A Survey of Botnet Technology and Defenses,” 2006.