ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Reviewing Anatomy of Botnets and Botnet Detection Techniques

Ramish Ahmad Zaidi
Department of Computer Science and Engineering
Jamia Hamdard
New Delhi, India

Safdar Tanveer
Department of Computer Science and Engineering
Jamia Hamdard
New Delhi, India

Abstract: Botnets are one of the biggest threat to the cyber world around from a last two decades and they are responsible for many cyber crime cases in recent times. A botnet is basically a network of malicious computers or devices which is controlled by a botmaster where victims remain unaware about it. In this review paper, we are going to analyze that how a botnet is created and how it can be controlled by an attacker. There are some techniques and methodologies that are also discussed which are used to know that how a botnet should be detected.

Keywords: botnet; botmaster; bot agents; command and control server (C&C); threat; honeynets.

I. INTRODUCTION

Today's world is hugely dependent upon internet. People are running businesses, doing many more things over internet because of the ease and benefits of the internet and modern technology like cloud computing which can use the storage provided by cloud and can access to that data again very easily from anywhere. Cloud computing gives many services which are exceptionally helpful to use. Truth be told, one can state that the entire world is presently in the cloud but some disadvantages are also there of this technology.

Internet can also be used in cyber crimes too by harming the confidentiality of the data and integrity of the data and by doing information security breaches, identification theft and many more attacks. Internet and Information security is a very big issue that the world is facing right now. Every government and organization is tensed about cyber security of their own.

Attacker spreads Trojans and malwares to increase number of bots in the network. Here bot is referred to robot and net is referred to network, so a botnet is a network of robots or computers or servers where the end user remains unaware of it but the attacker keeps controlling and gaining the access to all the systems of the network.

Attackers controlling botnets can use these bots remotely through command and controlling server. A command and control server is nothing but itself one the bot of the same botnet where attacker uses this bot to control and communicate other bots through commands. A bot master can use a single bot as well as many bots at a single time through commands. The size of a botnet can be increased by compromising more devices or servers into the network. Botnet has the property of propagation [1].

Types of attacks happen by botnets are mostly DDOS, phishing fraud, click fraud, password stealing, spamming, bit coin fraud, mass identity theft, sniffing traffic, spreading new malware and key logging [1].

Compromised systems in the botnet are also called as zombie, hence botnet is called as zombie network.

The first five years was crucial in the making of botnet. During 1993's, the attackers created the first botnet which was named as "Eggdrop". After that attackers created more advanced botnets with new functions and features. Up to 2002, many new botnets were created. These were the years when most attackers started to use botnets and hence the number of cyber attacks increased rapidly.

II. LIFE CYCLE OF A BOTNET

A new bot can be added in a botnet only through a procedure called botnet life cycle. This life cycle contains different phases for making a botnet or increasing a botnet. Different researchers suggests differently about botnet life cycle.

There are three different phases in a lifecycle of a botnet. These three phases are injection and infection phase, command and control phase, and botnet application phase. However, this suggestion is not considered as the best suggestion about the phases of a botnet life cycle [1, 2].

According to other researchers, [3] suggested that there are five phases in a life cycle of a botnet: Initial infection, secondary injection, connection, sending malicious code, and maintenance and updating.

When a new device which is connected to the internet is infected by a botnet, then it is been injected with a particular type of malicious code into the system through protocols like HTTP, FTP and P2P which connects the new infected system to the command and .control server of the botnet. Once this malicious code is injected into the system, the system starts working as a zombie computer for the botnet. The attacker can now control the new victim by sending commands through its command and control server. For continuous proper working of the botnet, their masters keeps them updated and maintained [1, 4].

III. BOTNET TOPOLOGIES

Network topologies do matters when talking about botnet because they can make a great difference in the performance of a botnet. Attackers have been using botnet with different topologies and architectures time to time. "Ollmann" [5] suggested the four main topologies that are used in botnets.

A. Star Topology

This type of topology provides botnet a very good bot management system and communication system between bots. Despite all, this topology has a big disadvantage that it only has one C&C server.

So it faces the problem of single point of failure i.e. however, if the C&C gets blocked then the whole network goes down. Even the legitimate user of the system can block connection from botnet themselves [5]. Figure '1' is describing Star topology with an Example.

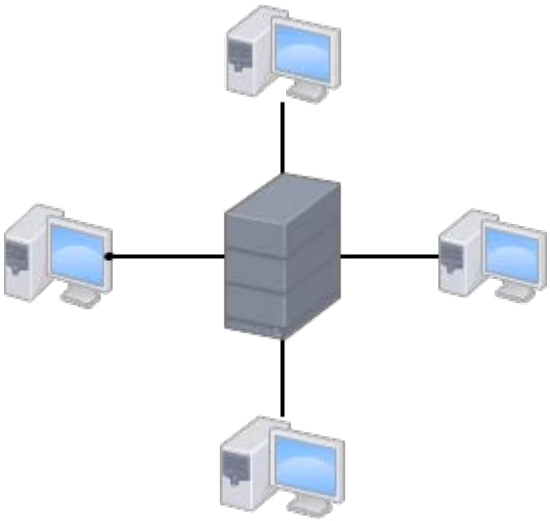

Figure 1. Example of a Star Topology.

B. Multi-server Topology

There are multiple servers or C&C that controls and manages the whole network and there is a better communication system between all the C&C and bots in this topology. If one C&C fail due to some reasons even then all other C&C still works and they makes decisions about the removal of the failed C&C. Here by having multi-server topology, the problem of single point failure gets eliminated [5]. Figure '2' is describing Multi-Server Topology.

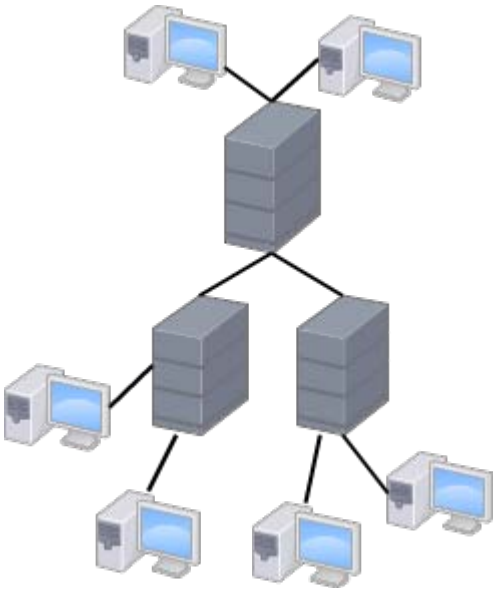

Figure 2. Example of a Multi-Server Topology.

C. Hierarchical Topology

A botnet based upon hierarchical topology has multiple C&C servers which are organized in groups to provide more reliability. Due to hierarchical topology of a botnet, it becomes easy to an attacker lease bots on rent. There are many benefits to use a botnet with hierarchical topology.

These types of botnets are also not easy to detect. In hierarchical topology based botnets, bot agents remains unaware from the location of other bot agents which makes it difficult to detect as well as it do not reveals the size of a botnet [5].

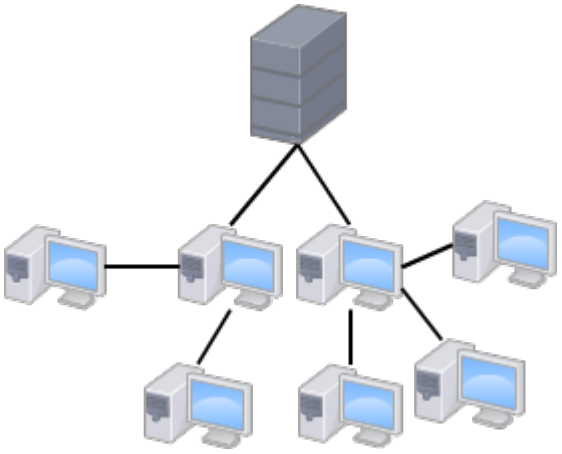

Figure 3. Example of a Hierarchical Topology.

D. Random Topology

This type of topology lacks of a centralized C&C infrastructure where the malware still spreads through the same procedures from botnet agents. Every zombie computer can act as a C&C server as per the conditions. There are now many paths and ways through which bots can communicate. Botnets of this topology are very tough to control and detect as there is no centralized C&C infrastructure i.e. if one serever is hijacked then the network will work with a new C&C server and the hijacked C&C server will be removed from the network. However, the time taken by bots to respond onto a command given by C&C is recorded higher than other topologies. But this topology provides many better features and functions than other topologies of botnet [5]. Figure '4' is describing Random Topology.

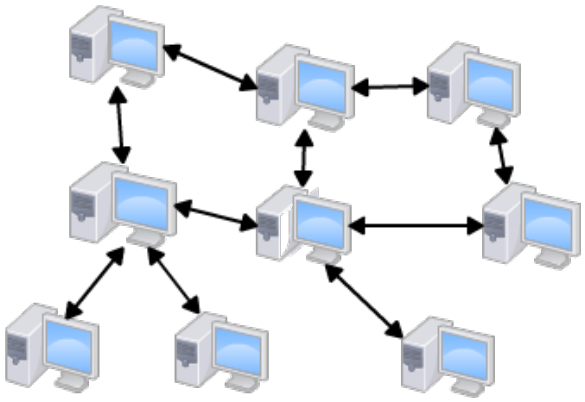

Figure 4. Example of a Random Topology.

IV. BOTNET DETECTION

Regarding botnet detection, still we don't have enough information and effective ways of detection. Botnets and their threats are not new and now they are pretty old, but there is still very much to research about them to keep them in control [3]. However, conditions are changing now and a lot of work is being done about the detection issue of botnets.

Many researchers up to now have researched about botnets and their detection techniques. These people have suggested bit differently from each other about botnets. However it is considered that to detect and to monitor a botnet, there are two main approaches [3, 6].

The first approach is to setting up honeynets into the systems and networks. The purpose of setting up honeynets is to gather information about botnets and to understand their behavior. Honeynets may not detect the botnet but it will understand the characteristics of it which may come in use to create more resistance against botnets [7, 8].

The second approach for botnet detection is based on passive network traffic monitoring and analysis. According to [3], there are three techniques of this approach to detect a bonet which are as follows:

A. Signature-based detection

This technique looks for signatures of botnets in order to detect them. Applying this technique is easy and it provides crucial information about the type of attack. Percentage of detection is very high and mostly it detects true botnet interfere. It has one drawback that only already known botnets can be detected using this technique [1, 3].

B. Anomaly-based detection

This detection technique helps to detect botnets through some network traffic anomalies [3]. It analyzes the entire network and always looks for any unusual behavior of the traffic across the network. This technique also overcomes the problem of not detecting unknown bots. It can detect those botnets even who has not been used even once in attacks. This detection is a bit costly but it performs very well and better than signature-based detection technique.[1].

C. DNS-based detection

Unlike signature and anomaly based detection techniques, the Domain Name Server (DNS) based detection technique is one in which only the information about DNS is used to detect that if there any botnet related with this DNS. However, there is a similarity between DNS based detection and anomaly based detection as the algorithms of anomaly based detection technique are also applied to DNS traffic [3].

V. CONCLUSION

Internet is becoming more common day by day and in fact it is being in use globally by millions of users on a large scale. The need of internet is increasing as well as the threats of internet are also increasing. With time, new threats are emerging on internet to attack users. After a bit old history of botnets, even still now best detection techniques have not emerged. This issue of botnet detection still needs to be researched as attackers comes with different functions of botnet every time.

In this paper, we have analyzed about botnets, lifecycle of a botnet, how they are created, how they are run to attack, in what kind of attacks they can be used and how to detect them. We analyzed how topology makes the difference in the performance and functions of a botnet. Attacks are being carried out by botnets very frequently now, so researchers still needs to find more effective ways to stop botnet attacks.

VI. 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.