Vandana Publications
IJEMR

Volume-8, Issue-4, August 2018
International Journal of Engineering and Management Research
Page Number: 193-195
DOI: doi.org/10.31033/ijemr.v8i4.13240

# Understanding the Botnet Phenomenon

Dr. Priyanka Surendran
Assistant Professor, Department of Business Informatics, AMA International University, BAHRAIN

Corresponding Author: spriyanka78@gmail.com

**ABSTRACT**

**Internet threats have increased manifold with the arrival of botnets. Many organizations worldwide and the social networks have been affected by botnets. Numerous researches have been carried to understand the concept of bots, C&C channels, botnet and botmasters. These botnets have been able to update itself regularly which makes them very difficult to be detected. The purpose of this paper is to understand the  of behavior of botnets and its affect on the virtual world. The paper has also analyzed the types of botnets, lifecycle and elements of botnets.**

**Keywords--** Bots, Botnet, C&C, Botmaster

## I. INTRODUCTION

Internet related crimes have evolved over a period and has been changing from attacks on the infrastructure to becoming real threat for people and organizations. One of the biggest threats that people and organizations are facing is the large collections of machines which has been infested by malware. A Botnet has been defined as a network which is comprised of machines which has been affected by malware. Botnets has become one of most dangerous and popular types of internet crimes. According to a study[2] about 16-25% of the computers on the internet are infected by botnet. Botmaster remotely controls the machines through a command and control channel(C&C).[1]The compromised machines are called bots. The C&C channel facilitates communication between botmaster and individual bots. The botmaster can control the machines to perform criminal activities like information and identity threat, Denial of service attacks(DoS)[3], unsolicited messaging etc[3].Many organizations and government agencies worldwide are trying to combat botnets through laws, regulations and other methods

It has been observed that botnet attacks are not confined to computers only. Smartphone have also become a target wherein the Bluetooth is being used as the command and control channel. Botnet has caused huge financial losses worldwide for companies, home users, government and internet service providers.

### *1.1 History of Botnet*

The study of the past history of bots and botnets provides interesting information. It was found that earliest way of using bots was in Internet relay chat(IRC)[4] channel management[4].IRC is a text based messaging system which was organized communication in channels. Users can join any channel and communicate with other users. The main role of botnet was to control interactions in the chat rooms. One of the earliest known bots was Eggbot[5] which was published in 1993.The IRC bots was used to attack other IRC users and servers. These were also used in Denial of service(DoS) and Distributed denial of service attacks(DDoS)[6].

### *1.2 Elements of Botnet*

The operation of Botnet can be better understood by the elements in a botnet. The elements of botnet are shown in figure 1.

- An executable file which will be present in a host that can perform a series of malicious actions is called bot. The bots can get installed through different ways including viral mechanisms and through infected sites. The bots are initialized every time that an infected machine is started.

The actions are performed through command and control infrastructure which is controlled by the botmaster

- The command and control(C&C) infrastructure is made of bots and a control entity which can be centralized or decentralized. The C&C infrastructure controls the bots in the botnet and maintains the connection in the infrastructure. [7]
- Botmaster is the machine that controls and configures the bot. It contains a machine which

installs the malicious bot, control and directs the bots when it joins the channel.

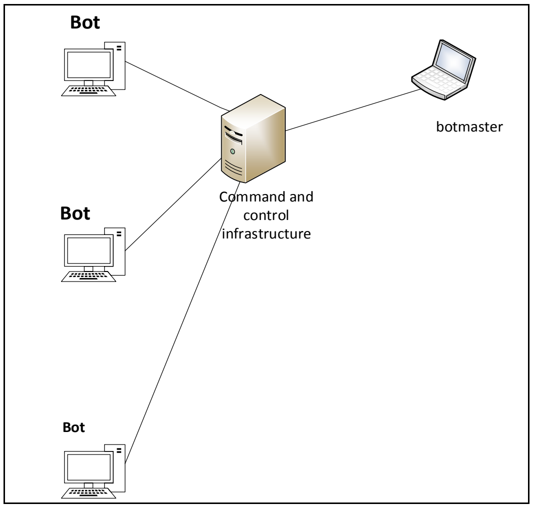

Figure 1: Elements of botnet

### *1.3 Botnet Lifecycle*

A botnet is created and maintained in five stages which are: Initial infection, Secondary injection, connection, malicious command and control, update and maintenance [6]. The figure 2 given below depicts the lifecycle of botnet.

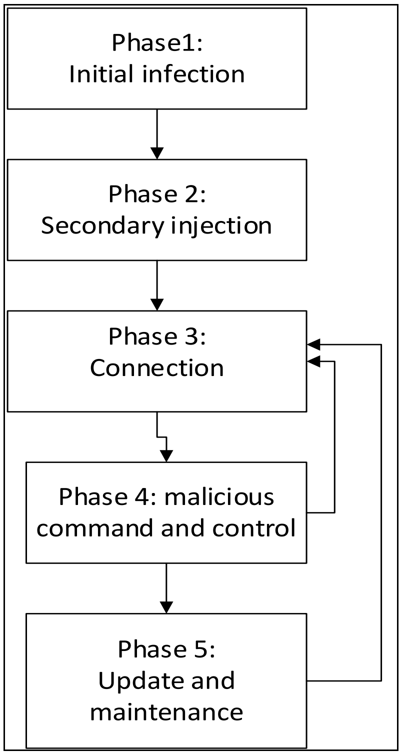
Phase1: Initial infection
Phase 2: Secondary injection
Phase 3: Connection
Phase 4: malicious command and control
Phase 5: Update and maintenance

Figure 2: Botnet lifecycle

In the Initial infection phase, targets are checked for any vulnerability. The attacker then attacks the victim machines through different methods like downloads of infected files, email attachments etc[6]

In the secondary injection phase, the infected hosts execute a script called shell code. When the code is executed, they make these hosts behave as bots. These codes get the image of the actual bot binary using protocols like FTP, HTTP or P2P. The code starts automatically when the infected machine is rebooted. The infected machines starts behaving like a "zombie" or real bot once these bot application are installed. [9, 10]

In the connection phase, the C&C channel is implemented by a bot program. The bot is connected to C&C Channel. The zombie becomes a member of the attacker's botnet army[10,11].

Once the connection is over, the malicious command and control activities will start. The botmaster uses the C&C channel to relay the commands to the bots. The C&C channel allows the botmaster to control the action of the bots to perform malicious activities [10, 11]

The final stage of the bot life cycle is the maintenance and updating of the malware. It is important to perform maintenance if the bots have to be kept in control. Maintenance involves code updating which could help in avoiding detection, adding new features or migrating to new C&C [10, 11, 12]. The migration to new C&C is very important in the survival of the botnet [9, 10, 13, 14]. The botnets avoid detection by using Dynamic DNS(DDNS)[15] which allows frequent updates and changes in server locations. In case the C&C server at a certain IP address is detected, another C&C can be set up easily with the same name at a different IP address. The new IP address can be easily sent to bots by short time-to-live(TTL)values for the domain names by the DDNS providers. The bots will shift to the new C&C and will stay alive[14,16,17]

## II. TYPES OF BOTNET

The botnets can be classified mainly based on two factors:

- Architecture
- Network protocols

### *2.1 Based on Architecture*

There are basically two known architectures for botnet which are centralized and decentralized.

**Centralized botnet:** In this architecture all the bots are connected to single C&C. The command and control channels awaits the bots to connect, register, track their status and send commands through the botmaster[18]

**Decentralised or P2P (peer-to-peer) botnet:** The bots are connected to different infected machines than to C&C. Commands will be sent from bot to bot. Each bot will have a set of neighbours and the command received by a bot from one of its neighbours will be sent to others. [18]

### *2.2 Based on Network protocols*

The botnet can be classified based on the network protocols:[18,19]

**IRC (Internet relay chat)-oriented:** Bots that are controlled using IRC channels. [18,19]

**IM(Instant messaging)-oriented:** The communication channels used here provided by instant messaging like AOL, ICQ etc[18,19]

**Web-orientetd:** A pre-defined web based server is connected to the bot. The bot sends the commands and transfers data through it[18,19]

**Other:** The other botnet connects through own protocoal based on the TCP/IP stack[18,19]

## III. CONCLUSION

Numerous researches have been conducted on the phenomenon of botnets. Botnets have been playing out as a significant threat all around the world. Botnets have been increasing with increase in the connectivity and the numbers of devices which are in the virtual world.

This survey aims to identify the phenomenon, review and understand the various aspects of botnets based on available researches. The paper aims to provide an understanding about the history, elements, types of botnet and botnet lifecycle. All these different aspects of botnet are discussed at length in this paper.

The study was restricted in understanding the different aspects of botnets. Further researches could be conducted level of the security threats posed by these botnets.

## REFERENCES

[1] E. Cooke, F. Jahanian, & D. McPherson. (2005). The zombie roundup: understanding, detecting, and disrupting botnets. *In: Proceedings of the Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop, USENIX Association, Berkeley, CA, USA*, 39-44.

[2] K. Birman, M. Hayden, O. Ozkasap, Z. Xiao, M. Budiu, & Y. Minsky. (1999). Bimodal multicast. *ACM Transactions on Computer Systems*, *17*(2), 41–88.

[3] P. Eugster, R. Guerraoui, S. Handurukande, P. Kouznetsov, & A. Kermarrec. (2003). Lightweight probabilistic broadcast. *ACM Transactions on Computer Systems*, *21*(4), 341–374.

[4] J. Oikarinen & D. Reed. (1993). *Internet relay chat protocol*. Available at: https://www.rfc-editor.org/rfc/pdfrfc/rfc1459.txt.pdf.

[5] *Eggdrop: Open Source IRC Bot*. (1993). Available at: http://www.eggheads.org/

[6] M. Feily, A. Shahrestani, & S. Ramadass. (2009). A survey of botnet and botnet detection. *In: Emerging Security Information, Systems and Technologies*, 268–273.

[7] M. Bailey, E. Cooke, F. Jahanian, Y. Xu, & M. Karir. (2009). A survey of botnet technology and defenses. *In: Conference for Homeland Security*, 299– 304

[8] SSC Silva, RMP Silva, RCG Pinto, RM Salles. (2013). Botnets: A survey. *Computer Networks*, *57*(2013), 378–403.

[9] M. Rajab, J. Zarfoss, F. Monrose, & A. Terzis. (2006). *A multifaceted approach to understanding the botnet phenomenon*. Available at: http://www.cs.jhu.edu/~fabian/papers/botnets.pdf.

[10] Z. Zhu, G. Lu, Y. Chen, Z. J. Fu, P.Roberts, & K. Han. (2008). Botnet research survey. *In: Proc. 32nd Annual IEEE International Conference on Computer Software and Applications*, 967- 972.

[11] K. K. R. Choo. (2007). Zombies and Botnets. *Trends and issues in crime and criminal justice, no. 333*. Available at: https://aic.gov.au/publications/tandi/tandi333.

[12] L. Song, Z. Jin, & G. Sun. (2011). Modeling and analyzing of botnet interactions. *In Proc. of Physica A*, *390*(2), 347–358.

[13] D. Dagon, G. Gu , C.P. Lee, & W. Lee. (2007). A taxonomy of botnet structures. *In Proc. 23rd Annual Computer Security Applications Conference*, 325-339.

[14] H. Choi, H. Lee, H. Lee, & H. Kim. (2007). Botnet detection by monitoring group activities in DNS traffic. *In: Proc. 7th IEEE International Conference on Computer and Information Technology*, 715-720.

[15] P. Vixie, S. Thomson, Y. Rekhter, & J. Bound. (1997). *Dynamic updates in the domain name system(DNS UPDATE)*. Available at: http://www.faqs.org/rfcs/rfc2136.html.

[16] D. Dagon, G. Gu , C.P. Lee, & W. Lee. (2007). A taxonomy of botnet structures. *In Proc: 23rd Annual Computer Security Applications Conference*, 325-339.

[17] R.Villamarin-Salomon & J.C. Brustoloni. (2008). Identifying botnets using anomaly detection techniques applied to DNS traffic. *In Proc: 5th IEEE Consumer Communications and Networking Conference*, 476-481.

[18] A. Karim, R. B. Salleh, M. Shiraz, S. A. A. Shah, I. Awan, & N. B. Anuar. (2014). Botnet detection techniques: review, future trends, and issues. *Journal of Zhejiang University SCIENCE C*, *15*(11), 943–983.

[19] F. Tegeler, X. Fu, G. Vigna, & C. Kruegel. (2012). Botfinder: Finding bots in network traffic without deep packet inspection. *In Proceedings of the 8th International Conference on Emerging Networking Experiments and Technologies*, 349–360.