ISSN : 2231-0711

A Survey on Botnets and Web-based Botnet Characteristics

Maryam Rahimipour[1]
[1]*Department of Computer Engineering*
Science and Research branch,
Islamic Azad university, Ardabil, Iran

Dr. Shahram Jamali[2]
[2]*Head of Computer Networks Lab*
Head of Computer Engineering and
Information Technology Department
University of Mohaghegh Ardabili, Iran

Abstract—**The biggest threat of the Internet, but little known to the general public is constituted by Botnets. Botnets are networks of compromised computers controlled under a common command and control (C&C) channel. Botnets are often used for malicious activities such as spam, click fraud, identity theft, phishing, and distributed denial of service attacks. Characterizing existing Botnets will help to coordinate and develop new technologies to face this serious security threat. In this work, we carry out an analysis of Botnets for Understanding the structure and lifecycle of Botnets, Variety of Botnets in terms of their topology and protocol used and then we highlight the web-based Botnet features for use in detection algorithms.**

Keywords—Botnet, command and control channel, Centralized, Decentralized, web-based Botnet.

I. Introduction

Today, Botnet is widely used in various cyber attacks which lead to serious threats to ours network assets and organization's properties. Botnet has become a widespread platform for malicious attacks and more new types of attacks are invented based on Botnets. Bots are used to carry out a wide variety of malicious and detrimental actions against systems and services: DoS attacks, spam distribution, phishing and click fraud, among others [1]. Botnets, or “Bot Networks,” are made up of large numbers of compromised computers that have been infected with malicious code, and can be remotely controlled through commands sent through the Internet under a common Command and Control (C&C) infrastructure [2]. Section II presents the Botnet structures. Botnet lifecycle are considered in Section III. BOTNET ARCHITECTURES are discussed in Section IV. Section V discusses Botnet communication Protocols. Web-based Botnet Features are discussed in Section VI. Finally, Section VII gives the overall conclusion of this paper.

II. Botnet structures

Botnet structures have three parts: Bot, Botmaster, command and control channel.

Bot – A Bot, emanating from the term ‘Robot’ which is also called as Zombie. It is a new type of malware installed into a compromised computer which can be controlled remotely by Botmaster for carrying out some orders through the received commands. After the Bot code has been installed into the seized computers, the computer becomes a Bot or Zombie. Contrary to existing malware such as virus and worm which their main activities focus on attacking the infecting host, Bots can receive commands from Botmaster and are used in distributed attack platform.

Botmaster: Botmaster is known as Botherder that is a person or a group of person which control and manage remote Bots and Botnet [3].

Command and control channel: The difference between the Botnet and the virus is whether it can be controlled or not [4]. Botnet use the command and control channel to control the Botnet. The most essential part of a Botnet is the so called command and control infrastructure (C&C). This infrastructure consists of the Bots and a control entity that can be either centralized or distributed. The C&C infrastructure typically serves as the only way to control Bots within the Botnet. The Bots are required to maintain a stable connection within this infrastructure in order to operate efficiently [2].

III. Botnet Lifecycle

A. Spreading and Injection

Botnets can come in different sizes or structures but, in general, they go through the same stages in their lifetime. The lifecycle of a Botnet begins with the infection process where the Botmasters use different methods and techniques such as malicious emails, Software vulnerability instant messaging to infect new targets and convert them into Bots [5].

B. Communications stage

The main difference between Botnet and other kind of malwares is the existence of Command-and-Control (C&C) infrastructure. The C&C allows Bots to receive commands and malicious capabilities, as devoted by Botmaster [3]. In other words during this stage the Bots listen to the C&C servers or connect to them periodically to get new commands from the Botmaster. A new command when detected by the Bots is treated as an order: they executed the order and the results are reported to the C&C server; the Bots then wait for new commands.

Botmaster must ensure that their C&C infrastructure is sufficiently robust to manage thousands of distributed Bots across the globe, as well as resisting any attempts to shutdown the Botnets.

C. Attack stage

The final goal of a Botnet is the execution of an attack. The Bots start to attack the targets according to the accepted commands. Sometimes, the Bots connect to a specially appointed server for the latest updates. The main feature of Botnet attacks is the enormous amount of attackers that take part on them [1].

Botnets are mainly created to carry out malicious activities in computer networks [6]. They are not only a dangerous threat to computer networks and the Internet, but are also involved in other types of threats and attacks [7]. Some examples of these attacks are listed as follows:

1) DDOS: Denial of service (DoS) attacks is attempts to prevent the legitimate use of a service or simply reduce its availability. Distributed DoS attacks (DDoS) are a particular case, in which multiple attacking entities operate simultaneously to attain this goal. Botnets fit perfectly for striking DDoS attacks [1]. As Botmasters control Botnets, they can carry out this type of attack from thousands of different places by sending a particular command to the Bots in the infected computers in the same Botnet [8, 9].

2) Spamming: Spam refers to unsolicited messages, which have the same content but are sent in high volume over different mediums like email, Instant Messenger, comments on blog or news groups [10]. Based on Kaspersky lab report [11] around 85% of spam activities are generated by Botnets. Therefore Botnets can be considered as the main platform to collecting different email addresses from infected computers and generate and send spam messages. Each Bot can send an average of three spam emails or fake messages per second [12].

3) Thieving Personal Information: Botmasters use the Botnets to steal information and use them for their own benefit. They can set a trigger to Bots and make them scan websites where important information is entered [7]. In addition, other applications such as key-loggers are spread by Bots to obtain important information like personal passwords and financial data like online banking [13, 12].

4) Illegal Hosting, Sale or Rent Services: A computer or server with a large storage and a high-bandwidth connection to the Internet can become a target for a Botmaster to gain control and use for file sharing and illegal hosting [12]. Botnet programs and hosting services are available for sale or rent for the malicious purposes in any required duration. One of the intentions of these services is to place further barriers and gaps between their customers and law enforcement [10, 14].

5) Click Fraud and Adware: One of the main differences between Botnets and other Internet threats is that a Botnet can be used to make money by click frauding. Botmasters can earn a lot of money by using their Bots to click on open websites that pay a small sum of money for each visit to the website or for each click on the advertisement. Pop-up advertisements can also be downloaded, installed or displayed by Bots to force a user to visit particular websites [10].

In addition to the attacks discussed above, Botnets can be used to spread different types of computer threats in the form of viruses, Trojans, backdoors, worms, etc. This means that Botnets are not only a threat, but also a platform for the distribution of other malwares [12].

IV. Botnet Architectures

The Command and Control mechanism creates an interface between the bots, C&C servers and the Botmasters to transmit data among them. According this channel, there are three different Botnet architectures: the Centralized model, the Decentralized model and Hybrid model [15].

A. Centralized Model

A centralized topology is characterized by a central point forwarding messages among clients or publishing them. The master selects a host to be the contacting point of all Bots. It can be a compromised machine or a legitimate provider for public service. When the victim is infected it will 'connect' to the C&C server and then will wait or check for pending commands from the Botmaster [5]. Figure 1 shows the basic communication architecture for a Centralized model.

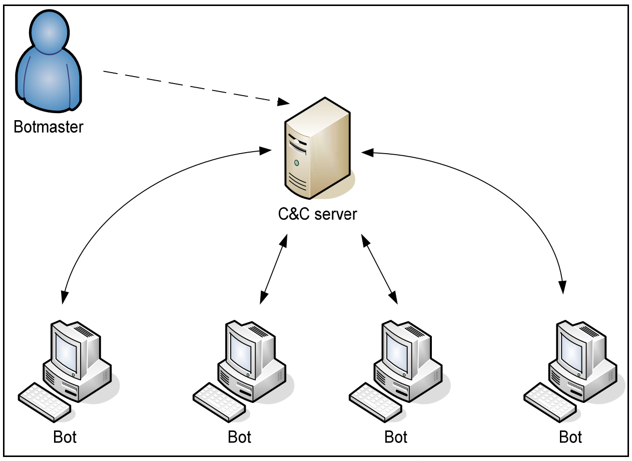

Figure 1: Command and control architecture of a Centralized model.

B. Decentralized Model

Botmaster can send commands from any peer. Botnets with a Random topology have no centralized C&C infrastructure. Instead, commands are injected in to the Botnet via any Bot agent. These commands are often "signed" as authoritative, which tells the agent to automatically propagate the commands to all other agents [3]. Figure 2 shows the architecture for a Centralized model.

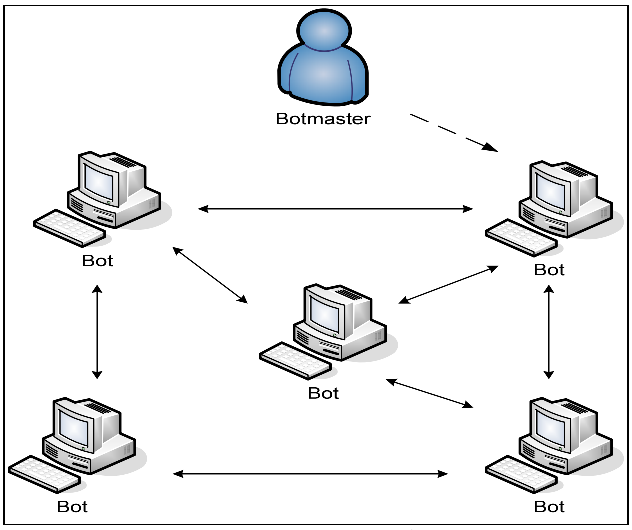

Figure 2: Command and control architecture of a Decentralized model.

C. Hybrid model

As discussed above, each C&C mechanism comes with a set of advantages and disadvantages with respect to the ease of use and management and difficulty of detection and abandonment. In order to take the advantages of each C&C model the different protocols and architectures are used to form a hybrid approach the hybrid approach is not limited to the use of certain services or architectures; in fact Botmasters can use any applicable protocols to implement this model as shown in Figure 3.

V. BOTNET COMMUNICATION PROTOCOLS

Botnet usually use well defined communication protocols. In [16], the communication protocols was be classified in three different categories.

1) IRC Protocol

This is the most common protocol used by Botmasters to communicate with their Bots. IRC protocol mainly designed for one to many conversations but can also handle one to one, which is very useful for Botmasters control their Botnet. However, security devices can be easily configured to block IRC traffic.

2) HTTP protocol

The HTTP protocol is another popular protocol used by Botnets which is difficult to be detected. Using the HTTP protocol, Botnet usually bypass security devices. The main advantage of using the HTTP protocol is hiding Botnets traffics in normal web traffics, so it can easily bypasses firewalls with port-based filtering mechanisms and avoid IDS detection.

3) P2P protocol

Recently, more advanced Botnet used P2P protocols for their communications [17].

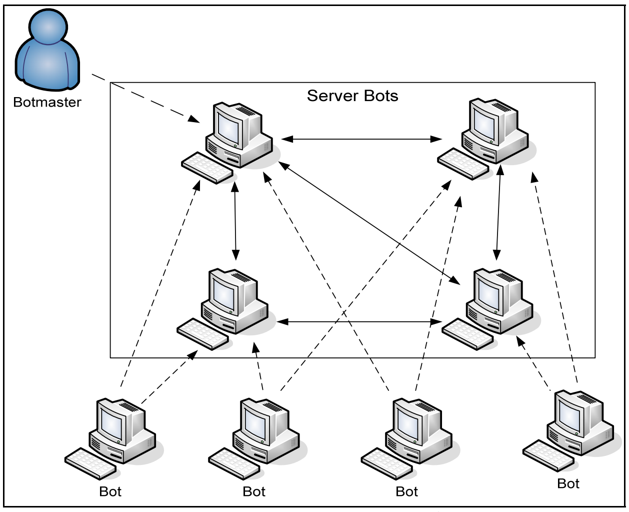

Figure 3: Command and control architecture of a Hybrid model.

VI. WEB-BASED BOTNET FEATURES

In recent years, Botnets use HTTP as communication protocol to command the victims. The web Botnets presented here differs from previous Botnets by employing HTTP protocol to proliferate virus. Although the HTTP Botnets have a good ability of self hiding, there are still some features that enable us to detect Botnets [18].

A. Header information

The HTTP header information generated by Botnet is often incomplete, even wrong whereas there must be much HTTP header information in the normal HTTP requests, such as user-agent [18].

B. Similar Communications density

In the command and control stage in Botnet lifecycle command and control servers and Bots have regular communications. This Communications can increase the density of network traffic [18, 19]. Figure 4 shows the increasing of network traffic during an attack. Also Figure 5 presents the count of similar request during command and control stage.

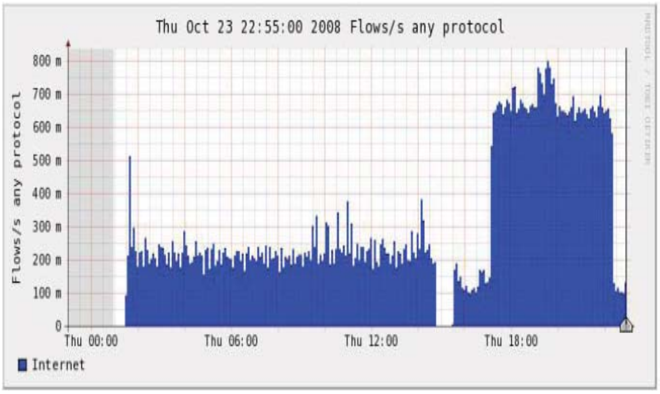

Figure4: Botnet flows during an attack [19].

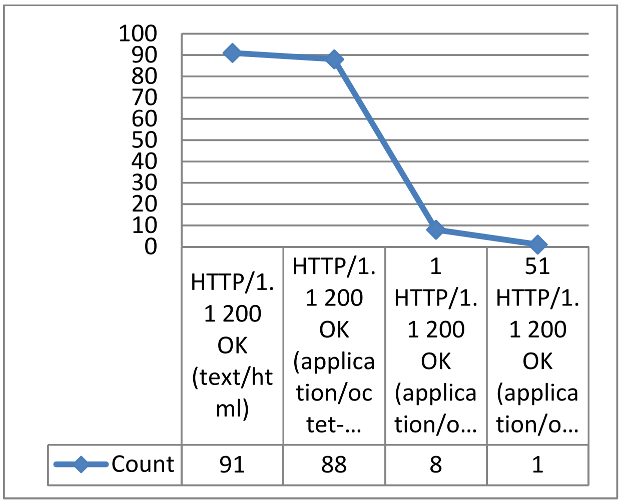

Figure5: count of similar request during command and control stage

C. Similar behavior

Botnets using HTTP with centralized structure share intrinsically and common key features. There are many common and group behaviors in the different stages of a Botnet, which are enumerated as follows: Emergence and spreading stage: Bots intent to infect other trusted hosts through scanning network, spreading worms and sending baleful e-mail. Also Bots belonging to the same Botnet have similar behaviors during a time window and this similarity continues during consecutive time windows as shown in Figure 6 [20].

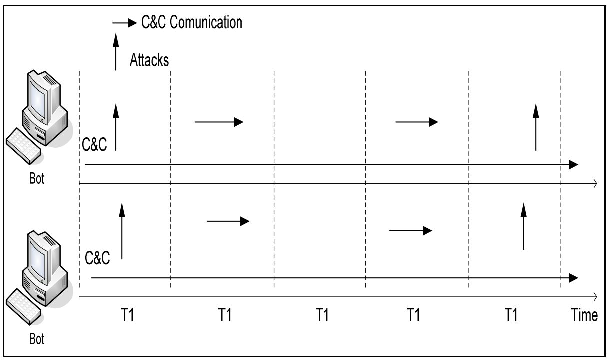

Figure 6: Similarity in bots behaviors in consecutive time windows [20]

D. Periodic behavior

Periodic behavior arises in Botnet C&C traffic due to the preprogrammed behavior in Bots. In many Botnet variants with different structures and communication protocols, Bots frequently contact each other every T seconds to receive commands, update data, and send keep-alive messages. This results in a periodic behavior in a host's traffic at the transport port number used by the Bot [21]. Figure 7 shows the time stamps of the similar requests in Botnet traffic.

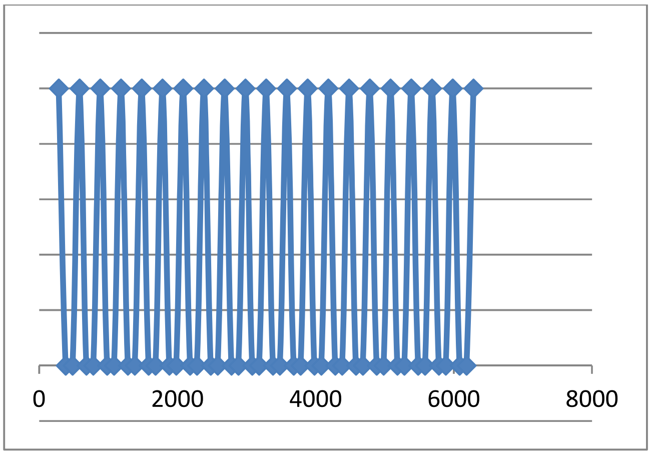

Figure7: Time stamps of similar requests

E. Response Time

Bots reply to the Botmaster's command very fast. In other words, human response to a command or request is always much slower than a Bot [22].

F. Commands Size

context length of normal web page will be relatively large. However, in order to prevent pressure to the server from a large flow, the instructions of the Botnet tend to be short [18]. The lengths of command packets are typically very small. Despite, the normal packets that have unbounded size, a typical command packet from Botmaster has a small size of 1KB or even less [22].

G. Instant Execution of Commands

Bots may launch an executable application on the infected host machine immediately after receiving Botmaster's command [22].

H. Hiding malicious traffic

Botmasters use HTTP protocol to hide their activities among the normal web flows and easily avoid current detection methods like firewalls. Because of the wide range of HTTP services used, unlike the IRC and P2P, it is not easy to block this service. Moreover, this service is commonly used by normal applications and services in the Internet [23, 12].

VII. CONCLUSIONS

As one of the most destructive and pervasive attacks on the internet, Botnet is a specific interest subjects for Network security researchers. Understanding the Botnet and its various features will lead to define new strategies and solutions to Botnet detections. In this context, we carry out an analysis of Botnets with two aim: 1) Understanding the structure and lifecycle of Botnets, Variety of Botnets in terms of their topology and protocol used. 2) Focus on the features of Web-based Botnet. in our study we highlight the web-based Botnet features for use in detection algorithms.

REFERENCES:

[1] Rodrıguez-Gómez, R. A., Maciá-Fernández, G., & Garcıa-Teodoro, P. (2011). Analysis of Botnets through life-cycle. In SECRYPT 2011-International Conference on Security and Cryptography.

[2] Upadhyaya, A., Jayaswal, D., & Yadav, S. (2011, April). Botnet: A new network terminology. In Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on (pp. 424-428). IEEE.

[3] Zeidanloo, H. R., & Manaf, A. A. (2009, December). Botnet command and control mechanisms. In Computer and Electrical Engineering, 2009. ICCEE'09. Second International Conference on (Vol. 1, pp. 564-568). IEEE.

[4] Cai, T., & Zou, F. (2012, September). Detecting HTTP Botnet with Clustering Network Traffic. In Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on (pp. 1-7). IEEE.

[5] Hachem, N., Ben Mustapha, Y., Granadillo, G. G., & Debar, H. (2011, May). Botnets: lifecycle and taxonomy. In Network and Information Systems Security (SAR-SSI), 2011 Conference on (pp. 1-8). IEEE.

[6] N. Hachem, Y. Ben Mustapha, G. G. Granadillo, and H. Debar, "Botnets: Lifecycle and Taxonomy," in Proceedings of the Conference on Network and Information Systems Security (SAR-SSI), 2011, pp. 1-8.

[7] M. Chandramohan and H. Tan, "Detection of Mobile Malware in the Wild," Computer, vol. 45, pp. 65-71, 2012.

[8] L. Chao, J. Wei, and Z. Xin, "Botnet: Survey and Case Study," in Proceedings of the Fourth International Conference on Innovative Computing, Information and Control (ICICIC), 2009, pp. 1184-187.

[9] E. Yuce, "A Literature Survey About Recent Botnet Trends," GÉANT Network, ULAKBIM,Turkey, Rep. JRA2 T4, 2012.

[10] C. Elliott, "Botnets: To What Extent Are They a Threat to Information Security?," Information Security Technical Report, vol. 15, pp. 79-103, 2010.

[11] V. Kamluk. (2009). The Botnet Ecosystem [Online]. Available: http://www.securelist.com/en/analysis/204792095/The_Botnet_ecosystem

[12] Eslahi, M., Salleh, R., & Anuar, N. B. (2012, November). Bots and Botnets: An overview of characteristics, detection and challenges. In Control System, Computing and Engineering (ICCSCE), 2012 IEEE International Conference on (pp. 349-354). IEEE.

[13] B. Stone-Gross, M. Cova, B. Gilbert, R. Kemmerer, C. Kruegel, and G. Vigna, "Analysis of a Botnet Takeover," Security & Privacy, IEEE, vol.

[14] Cisco, "Cisco 2009 Midyear Security Report: An Update on Global Security Threats and Trends," Cisco Systems, Rep., 2009.

[15] M. Bailey, E. Cooke, F. Jahanian, X. Yunjing, and M. Karir, "A Survey of Botnet Technology and Defenses," in Proceedings of the Cybersecurity Applications & Technology Conference for Homeland Security (CATCH), 2009, pp. 299-304.

[16] Taxonomy of Botnet Threats. Trend Micro Inc. White Paper,November, 2006.

[17] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon.“Peer-to-peer Botnets: Overview and case study,” In Proc. of ot Topics in Understanding Botnets (HotBots’07), 2007:198~201.

[18] Cai, T., & Zou, F. (2012, September). Detecting HTTP Botnet with Clustering Network Traffic. In Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on (pp. 1-7). IEEE.

[19] Chen, C. M., Ou, Y. H., & Tsai, Y. C. (2010, December). Web Botnet detection based on flow information. In Computer Symposium (ICS), 2010 International (pp. 381-384). IEEE.

[20] Arshad, S., Abbaspour, M., Kharrazi, M., & Sanatkar, H. (2011, December). An anomaly-based Botnet detection approach for identifying stealthy Botnets. In Computer Applications and Industrial Electronics (ICCAIE), 2011 IEEE International Conference on (pp. 564-569). IEEE.

[21] AsSadhan, B., Moura, J. M., & Lapsley, D. (2009, November). Periodic behavior in Botnet command and control channels traffic. In Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE (pp. 1-6). IEEE.

[22] M. M. Masud, T. Al-khateeb, L. Khan, B. Thuraisingham and K. W. Hamlen, “Flow-based identification of Botnet traffic by mining multiple log files,” in Proc. DFmA 2008, 2008.

[23] K. Tung-Ming, C. Hung-Chang, and W. Guo-Quan, "Construction P2P Firewall HTTP-Botnet Defense Mechanism," in Proceedings of the IEEE International Conference on Computer Science and Automation Engineering (CSAE), 2011, pp. 33-39.