A Survey of Botnet and Botnet Detection Techniques

Mitali Lade
Department of Computer Engineering
Shree L. R. Tiwari College of Engineering
Mumbai University, Thane,
Maharashtra, India

Dr. J. W. Bakal
Shivajirao S. Jondhale College of Engineering
Mumbai University, Thane,
Maharashtra, India

K. Jayamalini
Department of Computer Engineering
Shree L. R. Tiwari College of Engineering
Mumbai University, Thane,
Maharashtra, India

Abstract—Among the various types of malware, botnets are rising because the most serious threat against cyber-security as they provide a distributed platform for many illegal activities like launching distributed denial of service attacks against critical targets, malware dissemination, phishing, and click fraud. The defining characteristic of botnets is that the use of command and control channels through which they'll be updated and directed. Recently, botnet detection has been an interesting research topic related to cyber-threat and cyber-crime prevention. This paper is a survey of botnet and botnet detection. The survey clarifies botnet phenomenon and discusses botnet detection techniques. This survey classifies botnet detection techniques into four classes: signature-based, anomaly-based, DNS-based, and mining-base. It summarizes botnet detection techniques and provides a short comparison of botnet detection techniques.

Keywords— *Botnet; Botnet Detection;*

*****

I. INTRODUCTION

"Bots" under the remote control of a person's operator known as "Botmaster". The term "Bot" comes from the word "Robot"; and almost like robots, bots are designed to perform some predefined functions in automated way. In different words, the individual bots ar software programs that run on a host pc allowing the botmaster to control host actions remotely [1, 2].

Botnets pose a significant and growing threat against cyber-security as they provide a distributed platform for several cyber-crimes like Distributed Denial of Service (DDoS) attacks against critical targets, malware dissemination, phishing, and click fraud[3,4]. Botnet detection has been a major research topic in recent years. Researchers have proposed many approaches for botnet detection to combat botnet threat against cyber-security. in this survey, botnet phenomenon will be clarified and advances in botnet detection techniques are discussed.

This survey gives brief history on botnet detection. The remainder of the paper is organized as follows: Section II describes botnet phenomenon. In this
section, botnet characteristics and botnet life-cycle are explained to provide better understanding of botnet technology. Section III discusses different botnet detection techniques. Section IV discusses different schemes based on botnets for the analysis. Section V gives a comparison on these different schemes. The survey concludes in Section VI.

II. BOTNET PHENOMENON

Botnet has become a threatening phenomenon for the dissemination of various Internet attacks including spamming, distributed denial of service (DDoS) attacks, and malicious activities. Botnet is a network of infected machines (also called 'bots') which aims to disseminate malicious code over the Internet without user intervention. This process is carried out by a centralized entity called 'C&C', which is also called a 'botmaster'. Therefore, the theme of C&C mechanism is to increase the number of bot enemies and to coordinate among those enemies for the intensive destructive operations which are then carried out. The difference between a botnet and other types of network attacks is the existence of C&C. In addition, the infected machines (bots) receive instructions from C&C and act upon those instructions. The instructions/commands range from initiating a worm or spam attack over the Internet to disrupting a legitimate user request. Bots are computer machines with malicious software installed onthem, and they interact with an individual's machine without being noticed or even without any intervention by the user. A botmaster is the entity to whom all infected machines (bots) coordinate to initiate, manage, or suspend attacks. A botnet causes a number of serious offences on the Internet, as it allows intruders to hijack several computers simultaneously, which increases the number of cyber-attacks (Paxton et al., 2007). The research on the botnet is evolving rapidly because of the increasing curiosity in the Internet community. [3]

The concept of 'botnet' evolved in 1993 by introducing the first botnet called 'Eggdrop' (Wang, 2003). The history of botnets is highlighted in Table 1. The year field shows the

commencement year of each botnet, the 'number of estimated bots' refers to the number of bots anticipated in the given botnet attack, 'spam capacity' shows the number of attacks (per day) that hinders the services of legitimate users. Similarly, 'aliases' refers to the different naming conventions used by each botnet.[3]

Year	Name	Number of estimated bots	Spam capacity (billion/d)	Aliases
1993	Eggdrop	-	-	Valis
1998	GTBot NetBus	-	-	Aristotles
1999	!A	1 billion	-	-
2002	Sdbot/Rbbot Agobot	- -	- -	IRC-SDBot W32.HLLW.Gaobot, Gaobot
2003	Spybot Sinit	- -	- -	- Win32.Sinit, Troj/BDSinit
2004	Bobax Bagle	100 000 230 000	27 5.7	- Beagle, Mitglieder[4,5]
2006	Rustock	150 000	30	RKRustok, Costrat[6,7]
2007	Akbot Cutwail Srizbi Storm	1 300 000 1 500 000 450 000 160 000	- 74 60 3	- Pandex, Mutant Cbeplay, Exchanger Nuwar, Peacomm, Zhelatin[4,8,9,10]
2008	Conficker Maripos a Sality Asprox Gumblar Waledac Onewordsub Xarveste r Mega-D Torpig Bobax Lethic Kraken	10 500 000+ 12 000 000 1 000 000 15 000 n/a 80 000 40 000 10 000 509 000 180 000 185 000 260 000 495 000	10 - - - 1.5 1.8 0.15 10 - 9 2 9	DownAndUp, Kido - Sector, Kuku, Kookoo Danmec, Hydraflux - Waled, Waledpak N/A Rlsloup, Pixoliz Ozdok Sinowal, Anserin Bobic, Oderoor, Cotmonger None Kracken[4,11,12,13,14,15,16]
2009	Maazben Grum Festi BredoLab Donbot Wopla Zeus	50 000 560 000 n/a 30 000 000 125 000 20 000 3 600 000	0.5 39.9 2.25 3.6 0.8 0.6 n/a	- Tedroo Spamnost Oficla Buzus, Bachsoy Pokier, Slogger, Cryptic Zbot, PRG, Wsnpoem[17,18,19,20,21]
2010	Kelihos TDL4 LowSec Gheg	300 000+ 4 500 000 11 000+ 30 000	4 n/a 0.5 0.24	Hlux TDSS, Alureon LowSecurity, FreeMoney Tofsee, Mondera[4,22,23]
2011	Flashback	600 000	n/a	BacDoor.Flashback.39[24]
2012	Chameleon	120 000	-	-
2013	Boatnet	500+ server computers	0.01	YOLOBotnet[25]
2016	Mirai (malwar)	380,000	-	None

TABLE-I BOTNET HISTORY

A. Botnet Characteristics

Like the previous generations of viruses and worms, a bot is a self-propagating application that infects vulnerable hosts through exploit activities to expand their reach. Bot infection methods are similar to other classes of malware that recruit vulnerable systems by exploiting software vulnerabilities, trojan insertion, as well as social engineering techniques leading to download malicious bot code [26,27,28].According to measurement studies in [2] modern bots are equipped with several exploit vectors to improve opportunities for exploitation.

However, among the other classes of malware, the defining characteristic of botnets is the use of command and control (C&C) channels through which they can be updated and directed. The multi-tier C&C architecture of botnets provides anonymity for the botmaster. C&C channels can operate over a vide range of logical network topologies and use different communication protocols. Botnets are usually classified according to their command and control architecture [26, 27, 28, 29].

According to their command and control architecture, botnets may be classified as IRC-based, HTTP-based, DNSbased or Peer to peer (P2P) botnets [30]. P2P botnets use the recent P2P protocol to avoid single point of failure. Moreover, P2P botnets are harder to locate, shutdown, monitor, and hijack [31, 32]. However, according to the analysis in [26] the foremost prevalent botnets are based on internet Relay Chat (IRC) protocol [33] with a centralized command and control mechanism. IRC protocol was originally designed for large social chat rooms to allow for manykinds of communication and data dissemination among large number of end-hosts. the great prevalence of IRC-based botnets is due to the inherent flexibility and scalability of this protocol. furthermore, there are many open-source implementations that enable botmasters to increase them according to their demands [26, 34].

B. Botnet Lifecycle

Bots sometimes distribute themselves across the net by searching for vulnerable and unprotected computers to infect. once bot finds associate degree unprotected pc, they infect it so send a report back to the BotMaster. The bot keep hidden till they are conversant by their botmaster to preform associate degree attack or task. Fig.1 shows working of Botnet Detection Life cycle. Flow of life cycle is as given in following steps:

1. BotMaster uses a zombie (exploit machine) to send primary infection to the victim machine This can be done in form of sending email attachments.
2. Victim downloads the attachment and installs it on its machine so it gets compromised
3. The malicious bot program that has been installed onto victim's machine opens network ports for enabling secondary infection.
4. The victim machine downloads the secondary infection through which the machine becomes the a part of the botnet.
5. The victim machine is now programmed to periodically send its status information to the bot.
6. Bot controller sends a reply back to the victim and also sends new commands from BotMaster
7. .BotMaster sends commands to the bot controller which in turn passes to all the victim machine.

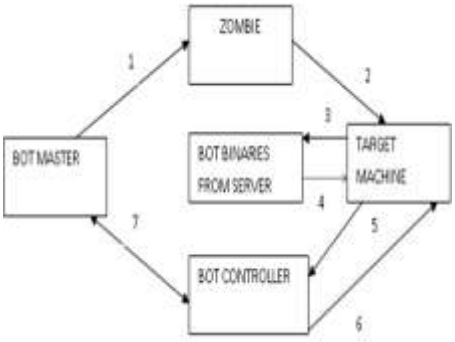

Fig:Botnet Life Cycle

III. BOTNET DETECTION

There are two main existing techniques to detect botnet they're as follows[2],[3],[4].

A) Honeynet: it's used to track and collect information of malicious activity. Honeynet is a set of Honeypots. A honeypot is bydesign insecure computational system that is placed in network with the objective of detection and capturing traffic from botnets. However Honeynet is usually used to understand the botnet characteristics but don't necessarily detect botnet and bot infection.

B) Passive network traffic monitoring: this method is useful to identify existence of botnet. Passive network traffic monitoring is
classified into five different techniques they're as follows; signature-based, anomaly based, DNS based, Mining, and Network based.

i)Signature-based detection technique

This technique is employed for detection of known bots. Detection of bots is based on previous knowledge about the botnet and malwares. so this solution is not feasible for unknown bots. Zero day attack can't be detected by this method. Rishi and Snort [3] tools are used to detect known bots and can applicable just for IRC protocol.

ii)Anomaly-based detection technique

Anomaly-based detection technique is based on several traffic anomalies like high network latency, high volumes of traffic, traffic on unusual ports, and unusual system behavior that might indicate the presence of malicious bot. Advantage of this method is that, it's used to detect unknown bot. Disadvantages of this method is that, it's used only for IRC protocol and it's not used to identify botnet C&C traffic because C&C traffic is not with high volume and doesn't cause high network latency.

iii)DNS based detection technique

This technique relies on DNS information generated by botnet. so it's possible to detect botnet DNS traffic by DNS monitoring by using the same principles of the anomaly based detection techniques. this

method will simply track DNS traffic anomalies. it's used to detect domain name with unusually high or temporally intense of DDNS query. Advantage of this detection technique is; it's used to detect DNS traffic anomalies

iv) Mining based

Mining based detection technique is used to detect the botnet by mining multiple log files. it's used to identify Botnet C&C traffic. this method includes machine learning process, classification of data, and clustering to detect botnet. Disadvantage of this method is that, it's difficult to detect botnet C&C traffic.

v) Network based

Network based detection technique is used to detect unknown, encrypted as well as protocol (IRC, http or P2P) and structure based botnet. This technique tries to detect Botnet by monitoring network traffics. Network based is classed in to two techniques; first technique is Active Monitoring; this technique intentionally injects test packets on to network to observe the flow of network traffic. Advantage of this technique is that the response time to detect malicious agents is less, it is simple technique and a drawback of this technique is; it will increase network traffic with additional packets sent to suspicious machines. Second technique is passive monitoring; it simply observes data traffic that is already on the network instead of injecting artificial traffic and look for suspicious communications (from bots and C&C servers).

V. COMPARISON OF DIFFERENT SCHEMES

This section provides a brief comparison of different botnet detection schemes. This comparison is summarized in Table 2 with its drawbacks.

Title of Paper	Findings	Drawback
[35] Building a scalable system for stealthy P2P botnet	In this they identifies all hosts that are likely part of P2P communication & then drives statistical fingerprints to profile P2P traffic & further it distinguishes between P2P traffic & legitimate P2P traffic	The system is not able to detect P2P bots IP
[36] Detecting stealthy P2P botnets using statistical traffic fingerprints	In this the system is able to detect stealthy P2P botnets even when the underlying compromised hosts are running legitimate P2P applications & P2P bot software	Drawback of this is that it gives negative impact on the resiliency of C&C infrastructure & limits the usability of entire bots even requires a lot of efforts for the design & operation of P2P botnets
[37] P2P botnet detection using network security	In this, Zeus banking Trojan is detected & deactivated by monitoring traffic & detecting most access unknown port	The system is working under web browser such as firefox or chrome, where identity of C&C infrastructure is not hidden. This makes quite easy to detect Bot from victim machine
[38] Detecting P2P botnets through network behavior analysis & machine learning	In this they detected P2P bots, which represents the newest & most challenging types of botnets currently available & studied the ability of 5 different commonly used machine learning techniques to meet online	Drawback of this paper is that none of these techniques can satisfy all the requirements of an online botnet detection framework

IV. RELATED WORK

From the past decade, the search for highly effective and efficient techniques of detecting botnet is a dynamic focus of research. The comprehensive works of [35] identifies all hosts that are likely part of P2P communication & then drives statistical fingerprints to profile P2P traffic & further it distinguishes between P2P traffic & legitimate P2P traffic. The extensive work of [36] detected stealthy P2P botnets even when the underlying compromised hosts are running legitimate P2P applications & P2P bot software. The great work done by [37] detected & deactivated Zeus banking Trojan by monitoring traffic & detecting most access unknown port. In [38] they detected P2P bots, which represents the newest & most challenging types of botnets currently available & studied the machine learning techniques to meet online botnet detection requirements.

	botnet detection requirements	

VI. CONCLUSION AND FUTURE SCOPE

As well discussed above since 1988, Botnet have evolved from the beginning assistant tool to the predominant threat in modern internet, in 1988 Botnet was not a malicious activity but later in 1998 , attacker use the bot to perform malicious activity via cyber crime. That is Botnets pose a significant and growing threat against cyber-security as they provide a key platform for many cybercrimes such as DDoS attacks against critical targets, malware dissemination, phishing, and click fraud etc. Although the number of bots to each Botnet seems to be decreasing, the monetary damaging power of the Botnets is continuously increasing given the development of internet bandwidth due to change in technology.

This paper described about Botnet and various Botnet detection techniques to detect the malicious activity and explained also some techniques to detect Botnet. Finally it is necessary to discuss about further Botnet developments which may arise in future. Hence the following idea summarize the future trends to be carried out in Botnet research ie Botnet can be detected by monitoring Traffic characteristics along using deep packet analysis. Botnet can be notable based on following reason, type of malicious activity perform by bots (click fraud attack, form Gabbing, information capturing, DDos etc.), Source and Destination IP address, Protocol used for attack (TCP, UDP, ICMP, HTTP or HTTPS), source and destination Port number , Date/Time and the architecture of the Bot and the technique required to implement this idea can be passive network monitoring.

ACKNOWLEDGMENT

I would wish to express my gratitude to my guide Dr. J.W Bakal and my co-guide Prof. K. Jayamalini for her instructive comments and valuable guidance. I am also grateful to all faculties of computer Engineering department, my colleagues and family for their encouragement and constant support.

REFERENCES

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

[2] M. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, “A multifaceted approach to understanding the botnet phenomenon,” in *Proc. 6th ACM SIGCOMM Conference on Internet Measurement (IMC’06)*, 2006, pp. 41–52.

[3] Karim, Ahmad, et al. "Botnet detection techniques: review, future trends, and issues." *Journal of Zhejiang University SCIENCE C* 15.11 (2014): 943-983.

[4] "Symantec.cloud | Email Security, Web Security, Endpoint Protection, Archiving, Continuity, Instant Messaging Security" (PDF). Messagelabs.com. Retrieved 2014-01-30.*[dead link]*

[5] Chuck Miller (2009-05-05). "Researchers hijack control of Torpig botnet". SC Magazine US. Retrieved 10 November 2011.

[6] "Storm Worm network shrinks to about one-tenth of its former size". Tech.Blorge.Com. 2007-10-21. Retrieved 30 July 2010.

[7] Chuck Miller (2008-07-25). "The Rustock botnet spams again". SC Magazine US. Retrieved 30 July 2010.

[8] Stewart, Joe. "Spam Botnets to Watch in 2009". Secureworks.com. SecureWorks. Retrieved 9 March 2016.

[9] "Pushdo Botnet — New DDOS attacks on major web sites — Harry Waldron — IT Security". Msmvps.com. 2010-02-02. Retrieved 30 July 2010.

[10] "New Zealand teenager accused of controlling botnet of 1.3 million computers". The H security. 2007-11-30. Retrieved 12 November 2011.

[11] "Technology | Spam on rise after brief reprieve". BBC News. 2008-11-26. Retrieved 24 April 2010.

[12] "Sality: Story of a Peer-to-Peer Viral Network" (PDF). Symantec. 2011-08-03. Retrieved 12 January 2012.

[13] "How FBI, police busted massive botnet". theregister.co.uk. Retrieved 3 March 2010.

[14] [13]"Calculating the Size of the Downadup Outbreak — F-Secure Weblog : News from the Lab". F-secure.com. 2009-01-16. Retrieved 24 April 2010.

[15] "Waledac botnet 'decimated' by MS takedown". The Register. 2010-03-16. Retrieved 23 April 2011.

[16] b c d Gregg Keizer (2008-04-09). "Top botnets control 1M hijacked computers". Computerworld. Retrieved 23 April 2011.

[17] "Botnet sics zombie soldiers on gimpy websites". The Register. 2008-05-14. Retrieved 23 April 2011.

[18] "Infosecurity (UK) - BredoLab downed botnet linked with Spamit.com". .canada.com. Retrieved 10 November 2011.

[19] "Research: Small DIY botnets prevalent in enterprise networks". ZDNet. Retrieved 30 July 2010.

[20] Warner, Gary (2010-12-02). "Oleg Nikolaenko, Mega-D Botmaster to Stand Trial". CyberCrime& Doing Time. Retrieved 6 December 2010.

[21] "New Massive Botnet Twice the Size of Storm — Security/Perimeter". DarkReading. Retrieved 30 July 2010.

[22] Kirk, Jeremy (Aug 16, 2012). "Spamhaus Declares Grum Botnet Dead, but Festi Surges". PC World.

[23] "Cómodetectar y borrar el rootkit TDL4 (TDSS/Alureon)". kasperskytienda.es. 2011-07-03. Retrieved 11 July 2011.

[24] "America's 10 most wanted botnets". Networkworld.com. 2009-07-22. Retrieved 10 November 2011.

[25] http://phys.org/news/2015-02-eu-police-malicious-network.html

[26] "Discovered: Botnet Costing Display Advertisers over Six Million Dollars per Month". Spider.io. 2013-03-19. Retrieved 21 March 2013.

[27] Honeynet Project and Research Alliance. Know your enemy: Tracking Botnets, March 2005. See http://www.honeynet.org/papers/bots/.

[28] G. Schaffer, “Worms and Viruses and Botnets, Oh My! : Rational Responses to Emerging Internet Threats”, *IEEE Security & Privacy*, 2006.

[29] E. Cooke, F. Jahanian, and D. McPherson, “The zombie roundup: Understanding, detecting, and disrupting botnets,”

in *Proc. Steps toReducing Unwanted Traffic on the Internet Workshop (SRUTI'05)*, 2005, pp. 39-44

[30] A. Ramachandran and N. Feamster, "Understanding the network-level behavior of spammers," in *Proc. ACM SIGCOMM*, 2006

[31] Z. Zhu, G. Lu, Y. Chen, Z. J. Fu, P.Roberts, K. Han, "Botnet ResearchSurvey," in *Proc. 32nd Annual IEEE International Conference onComputer Software and Applications (COMPSAC '08)*, 2008, pp.967- 972.

[32] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon, "Peer-to-peer botnets: Overview and case study," in *Proc. 1st Workshopon Hot Topics in understanding Botnets*, 2007.

[33] P. Wang, S. Sparks, and C. C. Zou, "An advanced hybrid peer-to-peer botnet," in *Proc. 1st Workshop on Hot Topics in understanding Botnets*, 2007.

[34] C. Kalt, "Internet Relay Chat: Client Protocol," *Request for Comments (RFC) 2812 (Informational)*, April 2000.

[35] A. Karasaridis, B. Rexroad, and D. Hoeflin, "Wide-scale botnet detection and characterization," in *Proc. 1st Workshop on Hot Topics in Understanding Botnets*, 2007.

[36] Zhang, Junjie, et al. "Building a scalable system for stealthy p2p-botnet detection." IEEE transactions on information forensics and security 9.1 (2014): 27-38.

[37] Zhang, Junjie, et al. "Detecting stealthy P2P botnets using statistical traffic fingerprints." Dependable Systems & Networks (DSN), 2011 IEEE/IFIP 41st International Conference on. IEEE, 2011.

[38] Y. Mane and K. Devadkar, "P2P Botnet Detection Using Network Security," in Proc. INTERFACE 2014 TEQIP-II Sponsored 3rd Int. Conf. on Network Infrastructure Management Systems, Mumbai, Jun. 2014.

[39] Saad, Sherif, et al. "Detecting P2P botnets through network behavior analysis and machine learning." Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on. IEEE, 2