World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:8, No:9, 2014

Categories of Botnet: A Survey

D. Seenivasan, K. Shanthi

***Abstract*—**Botnets are one of the most serious and widespread cyber threats. Today botnets have been facilitating many cybercrimes, especially financial, top secret thefts. Botnets can be available for lease in the market and are utilized by the cybercriminals to launch massive attacks like DDoS, click fraud, phishing attacks etc., Several large institutions, hospitals, banks, government organizations and many social networks such as twitter, facebook etc., became the target of the botmasters. Recently, noteworthy researches have been carried out to detect bot, C&C channels, botnet and botmasters. Using many sophisticated technologies, botmasters made botnet a titan of the cyber world. Innumerable challenges have been put forth by the botmasters to the researchers in the detection of botnet. In this paper we present a survey of different types of botnet C&C channels and also provide a comparison of various botnet categories. Finally we hope that our survey will create awareness for forthcoming botnet research endeavors.

***Keywords*—**Bot, Botmaster, Botnet, Botnet cloud, Mobile Botnet.

I. Introduction

A botnet is the collection of compromised computers which are controlled by the botmaster remotely via Command and Control (C&C) channel. The compromised system is termed as a bot which has vulnerabilities and paves the way for the invasion of the botmaster. The C&C channel can be used for communication between the botmaster and the individual bots in the botnet. The term “botnet” is a combination of “robot” and “network”. It performs malicious activities based on the command or script received from the botmaster through C&C channel. Botmaster can use legitimate web servers and protocols to conceal its presence from the intrusion detection mechanisms such as firewall. In this scenario it is very difficult to detect the botnet in the live environment and it costs more. The existing detection mechanisms are not compatible with the new trends of botmasters.

Recently, surfing the internet has become more dangerous, without the knowledge of security and its concerns. Criminals are using this slapdash attitude to dupe the victims by installing the malware onto their system. Botnet itself is not a malware and the network of computers with vulnerabilities indulges in malicious activities only after receiving the command from the botmaster, anytime from anywhere. Comparing with other existing malwares it is more dangerous because the masquerader can lease the botnet for cyber terrorism activities. Many organizations including Microsoft, DELL, McAfee, Kaspersky Lab, and social networks namely Facebook, twitter, Wikileaks and many other government agencies of developed countries namely FBI, Europol and the UK’s National Crime Agency (NCA) are still continuing their battle against the botnet worldwide through laws and regulations and many other measures. Henceforth, due to these curtailed activities by the developed countries, it is likely that the cybercriminals turn their tyrant face towards developing countries like India.

India ranks third among Zero Access botnet infected countries. While 35% of the infections were observed in the US, nearly 6% of Zero Access infections were in India, as per Symantec’s Internet Security Threat Report.

Recently, Botmasters are not only targeting computers but also Smartphones. They use Bluetooth as the command and control channel to create the mobile botnet which comprises of Smartphones, tablets and other PDA’s which are connected through Internet and wireless media.

Apart from using a network of infected machines, now botmasters can use Cloud services to build botnet and it is the most extreme challenge faced by the cloud service providers as it is hard to detect the botnet in a highly dynamic and heterogeneous environment.

The Botmaster utilizes the vulnerabilities of legitimate protocols like HTTP, FTP, P2P, ICMP, DNS, IRC and some of the IEEE standards like WiFi, Bluetooth, to make it as the C&C channel to bring all the bots under their control and hide their presence.

The most familiar mechanisms namely, BotHunter and BotMiner, to detect the botnet are mainly based on analyzing the traffic payloads and these techniques take more time, space and money. If the packets sent by the botmaster are encrypted, these techniques are not feasible and are not suitable to detect recent trends of botnet such as mobile botnet and bot clouds. Therefore, there is a need to restrain botnet which demolish the fruitfulness of the cyber world to the forthcoming generations.

II. Botnet – Life Cycle

A botnet lifecycle [1], [2] consists of four phases: initial formation, C&C, attack and post-attack. The initial formation phase is the first phase in which the botmaster exploits the vulnerabilities of a target system and infects the victim machine by injecting the scripts and makes the compromised computer as a bot which enables the bot to execute malicious code in the third attack phase. The bot will establish a connection to the command and control channel, then joining the botnet authoritatively in the second phase. In the attack

D. Seenivasan is with the computer science and engineering Department, Assistant Professor, from K. S. Rangasamy College of Technology, India (e-mail: seenivasand@ksrct.ac.in).

K. Shanthi is with the computer science and engineering Department, M.E. (CSE) Final Year, from K.S.Rangasamy College of Technology, India (e-mail: shanthikannappan@gmail.com).

phase, after launching a connection with the C&C channel, the bot will request for the command from the botmaster to begin the malicious activities. Typically, in the post-attack phase, updation of the scripts which is loaded in the initial phase can be done to defend against detection by the intrusion detection mechanisms.

III. Categories of Botnet – Based On C&C Channel

Botnets can be mainly classified into four types based on the C&C channel used. They are IRC (Internet Relay Chat) botnet, P2P (Peer-to-Peer) botnet, HTTP (Hyper Text Transfer Protocol) botnet and the hybrid botnet which is the combination of all types of Botnet Structures.

Recently botmasters use SMS and Bluetooth as the C&C Channel to conduct malicious activities in highly sophisticated mobile phones like Smartphones. Those botnets are known to be mobile botnets. Now Botnet can be implemented using Cloud mechanisms. Such botnets are known to be bot cloud or cloud based botnet. These categories are shown in Fig. 1. IRC and HTTP botnets have a centralized structure whereas P2P botnet follows a decentralized structure.

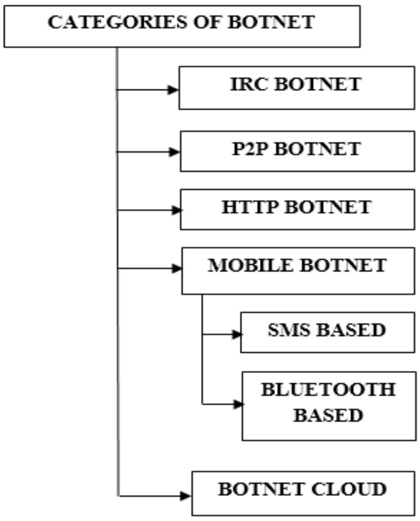

Fig. 1 Categories of Botnet

A. IRC Botnet

Botmaster exploits Internet Relay Chat (IRC) as the C&C Channel to communicate and control the bots. Initially IRC bots (e.g. egg drop) can be used to monitor and prevent malicious interventions into the IRC Channel and perform some automation tasking. It is the first kind of bot developed for a beneficial purpose. Later, it can be used for demolition activities.

Based on the commands received from the centralized IRC server, individual bots perform the malicious actions. The centralized Botnet structure is shown in Fig. 2. Botmaster can use the valid IRC ports to activate the bots through their commands/scripts. The heavy traffic of IRC servers makes the masqueraders' presence imperceptible. The entire botnet can be collapsed by simply shutting down the IRC Server.

IRC Botnet is otherwise known as push style model because commands are sent to the bots connected to the IRC Channel from the botmaster frequently.

Botmaster send's the command a normal chatting message. Before sending the command, the botmaster authenticates the username and password. After completing the authentication process the botmaster issues commands to the bot connected to the IRC channel to obtain the information about the bot. For Example ".sysinfo" command can be used to obtain the system information of the bot in the IRC Botnet.

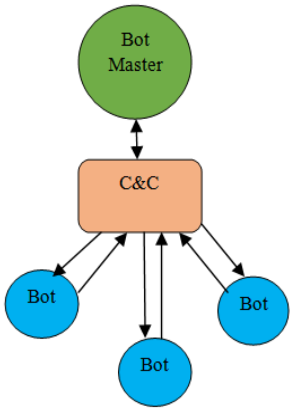

Fig. 2 Centralized Botnet Structure

B. Peer-To-Peer Botnet

P2P Botnet can be formed by using the P2P protocols and decentralized network of nodes. The decentralized/P2P Botnet structure is shown in Fig. 3. It is very difficult to shut down the P2P botnet due to its decentralized structure. Each P2P bot can act both as the client and the server.

The botmaster shares the command file with specific search key to each and every bot in the P2P botnet. The bots frequently communicate with each other and send "keep alive" messages and find the command file with the search key. P2P botnet are highly robust because the network is resilient. It has the only limitation of having a higher latency for C&C data transmission.

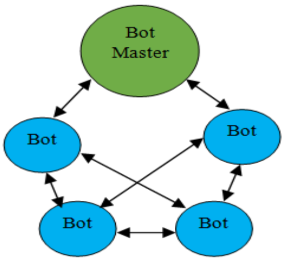

Fig. 3 Decentralized Botnet Structure

C. HTTP Botnet

HTTP Botnet is a centralized botnet, using HTTP protocol as the C&C server. Botmaster uses HTTP protocol to hide their activities among the normal web traffic and easily escape from current detection methods like firewalls and other Intrusion Detection Systems. The bots use specific URL or IP address defined by the Botmaster to connect to a specific web

International Science Index, Computer and Systems Engineering Vol:8, No:9, 2014 waset.org/Publication/10000001

server, which acts as the Command and Control Server at regular intervals defined by Botmaster. Instead of remaining in connected mode after establishing a connection like IRC bots, the HTTP bots periodically visit HTTP C&C server (certain web server) to get updates or new commands. This model is called the PULL style because commands are downloaded by bots periodically from the C&C server and the commands are stored in a file in the C&C server by the botmaster.

Cyber criminals used these HTTP based botnets to host the Phishing sites for the purpose of financial thefts. Some of the known HTTP based botnets are Bobax and ClickBot.

D.Hybrid Botnet

Basically Hybrid botnet is the combination of two or more botnet models such as IRC, P2P and HTTP botnets. It can follow both centralized and decentralized structures. The Hybrid Botnet structure is shown in Fig. 4.

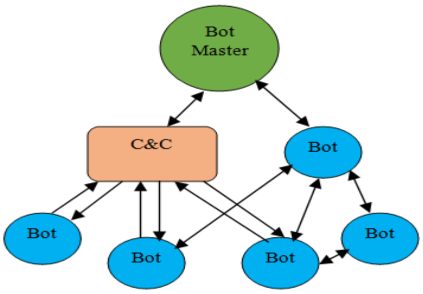

Fig. 4 Hybrid Botnet Structure

E. Mobile Botnet

Mobile botnet can be formed by exploiting the SMS and Bluetooth features of the mobile phones. Botmaster can use both the Bluetooth and SMS as the C&C channel through which it is possible to control the bots.

1) SMS Based C&C

The first and foremost SMS mobile botnet is iKeeB [3]. Botmaster utilizes SMS (Short Messaging Service) on smartphones and other mobile devices with such facility to transmit the malicious commands/scripts without the knowledge of the user. The advantage of SMS-based C&C is that the botmaster can easily communicate with the root node because of tree topology form of communication. In additional, SMS-based C&C has the disadvantage that SMS-based C&C needs a node list which is to be operated on infected mobile phones. SMS based C&C channel is considered to be the weakest when compared to other C&C channels because it makes it very difficult to manage all the bots of the botnet.

2) Bluetooth Based C&C

Botmaster can also utilize the vulnerabilities of Bluetooth technology and make it as the Command and Control (C&C) channel [4]. A Bluetooth based C&C is responsible for command transmission between the Bluetooth-enabled devices. It enables faster communication by simplifying the authentication and authorization process. After successfully completing the pairing process, a bond will be created between the two Bluetooth enabled devices which facilitates the construction of the Bluetooth C&C channel and makes the devices start the communication.

The vulnerabilities of Bluetooth technology allow constructing the stealthy C&C channel that can easily evade intrusion detection and enable operation in secrecy without the knowledge of the users. Besides the secrecy, Bluetooth C&C channel also offer some additional advantages. Firstly, the construction of a Bluetooth C&C will always be possible because Bluetooth technology is available in most of the devices. Secondly, the implementation of the Bluetooth C&C channel is cost free when compared to other C&C channels such as SMS or Internet. Finally, the Bluetooth C&C channel provides quick and cost free data communication. These advantages make the Bluetooth C&C channel to evade detection mechanisms.

The Bluetooth C&C channels also have some weaknesses. Firstly, the devices must be available in close proximity for the construction of the channel. The communication fails when the devices are out of range. Construction of the Bluetooth C&C channel is thus only possible when the devices are in close proximity and clustered together for a certain period of time. Secondly, Bluetooth technology consumes more battery power so that the Bluetooth C&C channel supports data communication for a short period and only very less amount of data can be transferred. If the Bluetooth is left for an indefinite period, the battery power of the device will completely deplete, causing the device to shut down and also destroy the Bluetooth C&C channel.

Besides having some disadvantages, the Bluetooth C&C channel is more ideally suited for command dissemination within a Mobile botnet than SMS based C&C.

F. Bot Cloud

Botmasters can use Cloud services to build botnet [5] and it is the most extreme challenge faced by the cloud service providers because it is hard to detect the botnet in a highly dynamic and heterogeneous environment. Such Botnets are known to be Bot clouds or cloud based botnet.

The main advantage of the botcloud over the traditional botnet is that it can be possible for the botmaster to fully utilize the resources without any interruption. The resources are always available online and ready to use. A botcloud can be constructed and be functional in a few minutes while a traditional botnet requires a lot of time for construction, waiting for days or months to take the control of the bots without the knowledge of the ordinary user. Finally a bot cloud can also be free from the risk of detection by security mechanisms.

G.Comparison

Comparison of different botnet categories is shown in Table I.

Comparison can be done based on C&C protocol/Channel, Structure, Strength and Weakness.

TABLE I
COMPARISON OF BOTNET CATEGORIES

Type of Botnet	C&C Protocol/Channel	Structure	Strength	Weakness	Examples
IRC	IRC	Centralized	Low latency communication, Flexible, Botmaster have Real time control over the Bots	The entire botnet can be collapsed by shutting down the IRC Server	GTbot, SDbot, Agobot, Spybot etc.,
P2P	WASTE, P2P, Self-defined	Decentralized/ Distributed (P2P)	Free from single point of failure, more robust	High Latency Communication	Nugache, Storm, etc.,
HTTP	HTTP	Centralized	Bots hide their communication flows in the normal HTTP traffic	Botmasters do not have real time control over the Bots; the entire botnet can be collapsed by shutting down the web servers	Bobax, Clickbot etc.,
Mobile Botnet (SMS Based)	SMS	Tree Topology	Communication realized in tree topology, Difficult to detect the bot communication	SMS-based C&C requires a node list to be operated on infected phones	iKee.B etc.,
Mobile Botnet (Bluetooth Based)	Bluetooth	Changing topology	Faster Communication, Data transfer is cost free	Difficult to construct the channel if the devices are out of range, Short data transfer due to consumption of more battery power	ZitMo
Bot Cloud	Cloud Resources	Changing Topology	Fully utilize the resources without interruption, Construction time is very less, Bot cloud is always online and ready to use	Weakness of Cloud Computing	-

IV. CONCLUSION

Today the great challenge faced by cyber security researchers is the botnet. Botnet itself is not a malware but can host malicious activities like DDoS attacks, click fraud, phishing attacks etc., by simply transmit the commands/scripts through the C&C channel to the bots. This paper mainly surveys categories of botnet based on C&C channel used by botmasters and also provide a simple comparison of botnet categories. We hope that it will create awareness about the botnet and pave the way for more researches in the field of cyber security.

REFERENCES

[1] David Zhao, IssaTraore, BassamSayed, Wei Lu, SherifSaad, Ali Ghorbani and Dan Garant,"Botnet detection based on traffic behavior analysis and flow intervals,"*Elsevier Computers & Security*, vol. 39, pp. 2-16,November 2013.

[2] Maryam Feily, AlirezaShahrestani and SureswaranRamadass," A survey of botnet and botnet detection," in*2009Proc.IEEE third international conference on emerging security information, systemsand technologies*, pp.268-273.

[3] Abdullah J. Alzahrani and Ali A. Ghorbani, "SMS mobile botnet detection using a multi-agent system: research in progress,"in*2014Proc. ACM ACySE1st International Workshop on Agents and Cyber Security*, no.2.

[4] Heloise Pieterse and Martin S. Olivier," Bluetooth Command and Control channel,"*Elsevier Computers & Security*, vol. 45, pp. 75-83, September 2014.

[5] Jerome Francois, Shaonan Wang, Walter Bronzi, Radu State and Thomas Engel, "BotCloud:Detecting botnets using MapReduce," in*2011 Proc. IEEE International Workshop on Information Forensicsand Security*, pp. 1–6.