International Journal of Pure and Applied Mathematics
Volume 119 No. 17 2018, 421-429
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

Botnet Life Cycle and Topologies

[1]Navin Dhinnesh A D C, [2]Sundareswaran N,
[1&2] Department of Computer Applications
Mepco Schlenk Engineering College, Sivakasi
[1]navindhinneshadc@mepcoeng.ac.in, [2]sundares@mepcoeng.ac.in,

Abstract: The current cyber world faces a huge threat from various forms of malware. One among them is Botnet. A Botnet is nothing but a network with compromised computers called the bots. The network will be connected to Internet, and is controlled by Botmaster. The Botmaster attack the network from a remote location. Now a day's Botnet is considered to be the most dangerous threat in the cyber attack. Botnet may execute in an automated manner, since they are already predefined. The cyber attack varies from phishing, moving files, etc. All these are possible by means of command and control (C&C) server [1]. Currently researchers are doing more research work associated with the topic of cyber offense. For preventing this Bots lot of techniques have been introduced. The author in this paper discusses the Evolution of Botnet, its life-cycle, mitigation, etc.

Keywords: Bot, Botnet, Robot, C&C server, Internet Relay Chat

1. Introduction:

The short form of Robot is called as Bot. Bot is considered to be small programs, using which once can control a computer at a remote location. Using malware bots, a computer can be made to be infected. Thus these computers which are infected in the network will form Botnets. The vital element of Botnet is the Command and Control (C&C) server. Botnet is a collection of computers, which are connected to the cyber world mainly for malicious cause. These Bots may rum automatically or they will be executing a task once they are given a precise input. Botmaster is the one who controls the Botnet. Naturally the Botnets are installed in the machines which are compromised. The identity of the Botmaster is not known since they hide their identity [2].

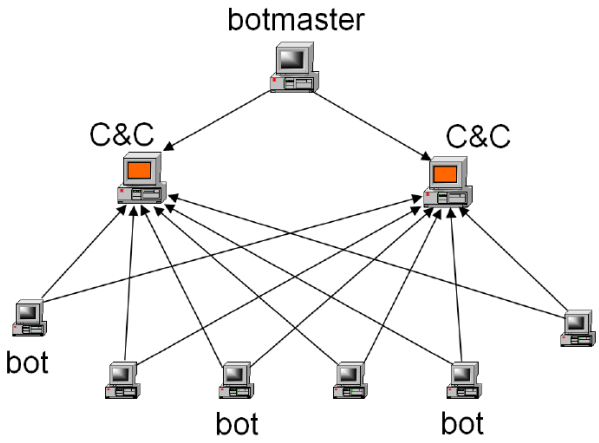

Fig 1. C&C architecture with bots

The Botmaster use few protocols for communication, especially to dominate the victim computer. The bots in the Botnet are controlled by C&C infrastructure (server). Two types of C&C architecture are available: i) centralized, and ii) decentralized. In the former, the client server approach is followed. The bot will be acting as a client and they will be contacting the central server for their commands. In the latter the bots are made to act autonomously. Recent Botnets are very much trained to handle huge bots [3]. The C&C architecture with the bot is shown in figure 1. The Botmaster sends the commands to the C&C servers. Once they receive the commands they send them to the bots. The Botmaster setup is shown in Figure 2.

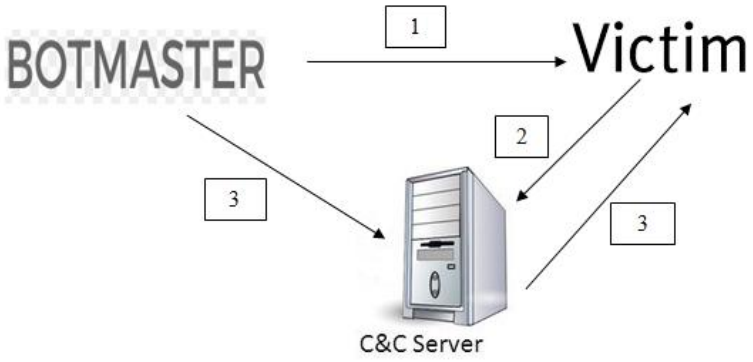

Fig 2. Botmaster setup

From the above figure 2, the Command and Control (C&C) server is explained as follows: 1. The Botmaster infects the victim with the Botnet, 2. now the Bot gets connected to C&C server, 3. Once the connection is established, immediately the Botmaster will be sending commands to the bot through C&C server, and 4. Now the steps are repeated. Soon the Botmaster has an army of bots to control from a single point

2. Centralized C&C Server

In C&C all the bots present are connected to the servers, hence the Botmaster can communicate with all the bots at the same time. After communicating with the bots, the Botmaster issue commands. Since the Botmaster are in direct contact with the bots, they can identify which bots are active or which one is in global distribution [4]. It is from Internet Relay Chat (IRC), the proposal of Botnet was initiated. IRC is considered to be a social chat which is text based, categorizes the communication in the form of channels [5]. The IRC protocol is considered a model for centralized communication. One to one (private) conversation is possible in this protocol. C&C are based on Hypertext Transfer Protocol (HTTP). The Botnets cannot be found out using Global Positioning System (GPS) for locating their positions [6].

3. Bot Life cycle

The life-cycle of a bot is shown in Figure 3. A total of 11 steps are involved in a life cycle. Starting with requirements and ending with Analyze the steps involves lot of stages. In requirement stage, the bot must know who the target is. What are the benefits the bot will get once it starts infecting? In spec stage, what are the things needed for the future must also be taken into consideration. Script engages in [7]constructing conversational scripts which are nothing but the interactions between users. Architect refers to two components: i) front end, and ii) back end. The latter is for translating the input from the user into precise actions. The former is for the computations being carried out by the bot.

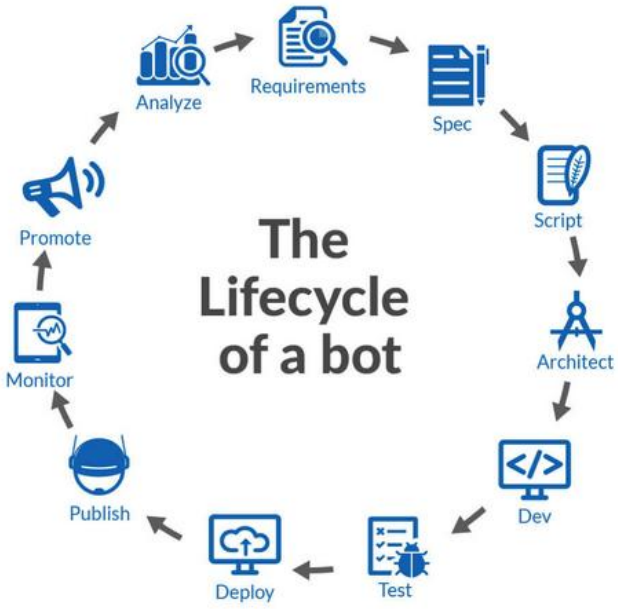

Fig 3 Life Cycle of a Bot

Courtesy [7]

Dev is where the exact bot is build up. Actual testing of the bots is done here. They have to be tested not in the emulator, but in real time scenario. Once the testing is over, the bot should be

deployed in a stable environment. After the process of testing and deployment, the bot must get approval from the app stores. After proper approval, if the bot is published, then it must be monitored continuously, i.e. the conversation of the user is monitored. [9] Our bot must be introduced to new users. The performance of the bot is to be analyzed as soon as it is being used. After proper analyze, the bot can be improved further. It is not an easy task for building a good bot. For a bot to become success, a lot of process needs to be done.

4. Botnet Topology

Depending upon the type of hijacking attempts or commercial defenses, C&C topologies are employed [8]. Using this topology one can reduce the system failure in the network. Four types of C&C topologies are i) star, ii) Multi-server, iii) Hierarchical, and iv) Random.

i) Star - This topology has a solo centralized C&C (CCC) source for communicating with each and every Bot agents. It is this centralized C&C issues every instruction to every Bot agents. Once the Bot agent infringes a computer effectively, it will automatically contact the CCC, upon which it will become a Botnet member and will look forward to the next instruction. Star C&C topology set up is shown in figure 4.

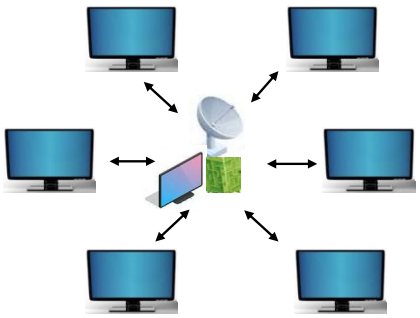

Figure 4: Star C&C topology setup

ii) Multi-server

This topology is an extension of the previous topology (Star). Here multiple servers are employed to issue the C&C instructions to the various bot agents. These servers communicate between themselves for managing the botnet. Constructing this setup is very complex one. But once constructed this setup can be used by star as well as multi-server topologies. Multi-server setup is shown in figure 5.

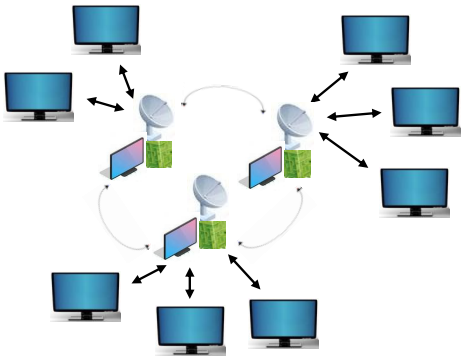

Fig 5. Multi-server setup

iii) Hierarchical

The single bot agent will not know the location of the complete botnet. This makes the researchers to guess the size of the botnet. Huge botnets are divided into sub botnets. Figure 6 shows the Hierarchical set up.

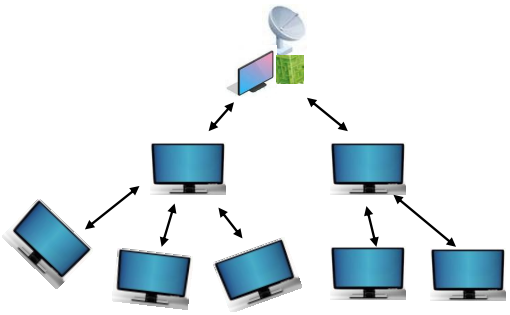

Fig 6. Hierarchical setup

iv) Random

Here there will be no centralized C&C set up. The bot agent will inject the commands into Botnet. These commands will be spread automatically to every agent. To communicate to the bot agents the random set up makes use of numerous message corridors. Figure 7 shows the Random set up.

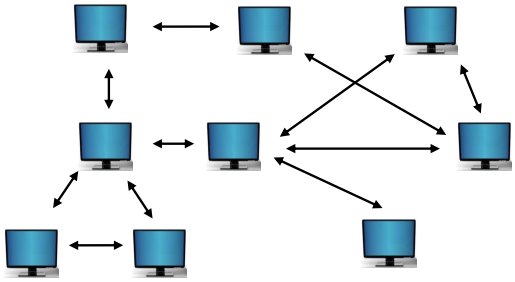

Fig 7. Random setup

Conclusion

Antivirus software is installed to avert the Botnets; also virus update is also being carried out to eliminate infected Botnets. Firewall in a system or an organization can be strengthened to control Bot attack. In the recent years cyber crime doers use Botnets as a familiar programs for attacking the user. The author says one must be well equipped from the future Bot attacks, since in future the Botnet attacks will be still very much dominant. Hence one must monitor those kinds of attacks and be prepared to develop programs that could destroy the Botnets.

ACKNOWLEDGMENT

The author acknowledges the support and encouragement by the Management, Principal and Director of Computer Applications department, towards this work.

Reference:

[1] A K Tyagi, G Aghila, "A wide scale survey on Botnet", International Journal of Computer Applications, Vol. 34, No. 9, November 2011

[2] https://security.radware.com/ddos-knowledge-center/ddospedia/botmaster/

[3] P Wang, S Sparks, C C ZouAn, "Advanced Hybrid Peer-to-Peer Botnet", IEEE Transactions on Dependable and Secure Computing, Vol. 7, No. 2, April - June 2010

[4] D Plohmann, E G Padilla, F Leder, "Botnets: Detection, Measurement, Disinfection & Defence", European Network and Information Security (ENISA), 2011.

[5] R Ferguson, "The Botnet Chronicles" , Trend Micro Whitepaper, 2010.

[6] Navin Dhinnesh ADC, "Global Positioning System – The Future", International Journal for Research in Emerging Science and Technology, Vol. 4, No. 8, August 2017

[7] https://chatbotsmagazine.com/the-bot-lifecycle-1ff357430db7

[8] K. Rajam, M. Chandramouleeswaran, Fuzzy Implicative B−Ideals Of B−Algebras, International Journal of Pure and Applied Mathematics, Vol 112 No. 5 , 149-157,2017.

[9] G Ollmann, "Botnet Communication Topologies, understanding the intricacies of Botnet Command-and-control", Damballa Inc., June 2009. Available online [http://technicalinfo.net/papers/PDF/WP_Botnet_Communications_Primer_(2009-06-04).pdf]