Scientific Journal of Impact Factor (SJIF): 4.72
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406
International Journal of Advance Engineering and Research Development
Volume 4, Issue 7, July -2017

A revise of botnets exploited in cyber world

Rathod Ravindra P[1], Shivpuje Prakash[2], Dr. S.D. Khamitkar[3]
[1, 2] School of Computational Sciences , S.R.T.M.Univerisity, Nanded (Maharashtra).
[3]GUIDE,S.R.T.M.Univerisity, Nanded (Maharashtra).

Abstract: *The botnet is still the challenging threat in cyber world. The botnet can spread from mobile to huge networks. This paper revises the botnets which exploited in cyber world. The botnet is now also used as cyber weapon for affecting government services, banking transactions, scientific laboratories, e-commerce sites, etc. The bot server uses command and control mechanism for controlling bot clients. The botnet can use different type of network topology. The most hazardous botnet uses the collaborative nature among the bot clients to hide identity in cyber world.*

Keywords: *Botnet; bot ;P2P botnet*

I. Introduction:

The botnet is network of bots. The bot is an infected host in network. The botnet can use different techniques to form a botnet like spyware, adware, malware, DDoS attack, Ransomware etc. The botnet controls the clients using mechanism known as command and control (C&C) mechanism. The bot server is also known as botmaster which issues command to gain control of infected host as bot. The botnet consist of hundreds to thousands of bot clients. Botnet is still the main focus of network security researcher because of its altering working mechanism. Every year new botnet arises with new type of working mechanism. Botnet is basically classified in three types as:

IRC (Internet Relay Chat) : This is old type of botnet used with IRC server.

HTTP (Hyper Text Transfer Protocol): This uses the HTTP for spreading the botnet.

P2P (Peer-to-Peer): This botnet uses the peer to peer protocols such as Gnutella. The P2P botnet operate in collaborative way to hide its identity. In this botnet each bot acts as server and client. There is no effect of single failure of bot on the botnet.

II. Major Botnets:

Following section reviews major botnets which became most affected the large number of hosts in cyber world.

1) SDBot: This bot was popular among the hackers as it was open source code kept on Internet. It is basically works using IRC Servers [12]. It searched only common vulnerabilities in hosts such blank passwords and open network share.
2) RBot: This botnet is more multifarious than SDBot. Its behaviour is changes with its new variants. RBot first started among botnet use of algorithms for encryption and compression. It depends on runtime executable programs such as PECompact or MoleBox. This botnet used for various illegal types of actions such as downloading files, getting serial keys, DDoS attacks or taking snapshots sing webcam. It scans TCP ports for open network shares to connect to vulnerable hosts.
3) Agobot: This botnet uses different step to spread its network. In fist step it enters the host using backdoor. Then it try to pause all security walls in attacked host. Last it takes control and stops all communication related to security. It can use the P2P network for attacking more hosts with speed of affecting hundred hosts at time. It also uses network share to spread in network.
4) Spybot: This is the next version of SDBot. It was also open source program like SDBot. It can use different techniques such as email spamming, key logging and data confine. It also scans TCP open ports and network shares. It also contains the list of possible system authentication usernames and passwords.

5) Peacomm : This is also known as Trojan.Peacomm which is P2P based botnet. It is based on overlay network method which uses Kademlia algorithm for distribution of nodes information. This botnet uses file which is executable on bot clients. After installing files it sends the messages to botnet for further actions.
6) Zeus/Zbot: This is largely admired in the hacker community as its main task related to theft credential information of banking and major ecommerce sites. It mainly attacked on Winodws hosts. There are many versions from open source to paid version. It includes separate control panel for performing attacks using web browser.
7) Stuxnet: This botnet was much highlighted in news because of its wide destroying capability. It searches vulnerabilities mainly though flash drives. It affected large number of industrial sector. The major attack was done on Iran's nuclear power stations.

III. Characterizations of revealing mechanism

There are many research has done in the detection of botnet in collaborative network of peers. Following table 1.1 shows the recent revealing mechanisms proposed by different researchers.

Table 1.1: Revealing mechanisms

Method used for revealing botnet	Botnet used	Botnet detection rate
Flow dependency in the traffic [1].	Synthetic P2P botnet traffic	100 %
Fuzzy pattern based filtering algorithm [2].	Honeynet used to collect bots	95.29 %
Data mining [3].	Trojan.Peacomm	98 %
Two stage Clustering and cross plane correlation [4].	Nugache and Storm	100 %
Contact tracing chain-based framework [5].	Simulation of botnet	90% - 100%
Classifiers (J48 and Random Forest) [6].	Storm and Waldac	100 %
Stream data classification and multi-chunk multi-level ensemble method (MCE) [7].	Nugache	95% - 100%
Machine learning classifiers [8].	Storm and Waldac dataset	98.1%
Correlation algorithm [9].	Peacomm	Approx 95% - 99.99 %
Multi-phased flow model [10].	SpamThru, Storm, Nugache	95%-100 %

From the above table it is clear that most of mechanism used known bots in collaborative network of peers such as Storm, Waldac, Nugache and Peacomm. The dataset such ISOT [11] as available open for research also include the botnet traces of known bots such as Storm, Zeus and Waldac. Some researchers also used the simulation based on the features of well-known bots [1][5][9].

Therefore, we can characterize the mechanism as follow:

a) Known bot based mechanisms
b) Anonymous bot based mechanisms
c) Simulation based mechanisms

IV. Conclusion:

The main hurdle in the collaborative network of peers is that there is no effect of single failure of bot in botnet as in IRC botnet. The known bot based mechanisms cannot detect new bots. But, the cyber attackers are using new propagation techniques for collaborative network of peers to avoid the detection. So, more research is required on revealing mechanism of anonymous bots.

REFERENCES

[1] Jiang, Hongling, and Xiuli Shao. "Detecting P2P botnets by discovering flow dependency in C&C traffic." *Peer-to-Peer Networking and Applications* 7.4 (2014): 320-331.

[2] Wang, Kuochen, et al. "A fuzzy pattern-based filtering algorithm for botnet detection." Computer Networks 55.15 (2011): 3275-3286.

[3] Lin, Shu-Chiung, Patrick S. Chen, and Chia-Ching Chang. "A novel method of mining network flow to detect P2P botnets." Peer-to-Peer Networking and Applications 7.4 (2014): 645-654.

[4] Gu, Guofei, et al. "BotMiner: Clustering Analysis of Network Traffic for Protocol-and Structure-Independent Botnet Detection.", USENIX security symposium. Vol. 5. No. 2. 2008.

[5] Huang, Zhiyong, Xiaoping Zeng, and Yong Liu. "Detecting and blocking P2P botnets through contact tracing chains." International Journal of Internet Protocol Technology 5.1-2 (2010): 44-54.

[6] Fedynyshyn, Gregory, Mooi Chuah, and Gang Tan. "Detection and classification of different botnet C&C channels." Autonomic and trusted computing (2011): 228-242.

[7] Masud, Mohammad M., et al. "Mining concept-drifting data stream to detect peer to peer botnet traffic." Univ. of Texas at Dallas Tech. Report# UTDCS-05-08 (http://www. utdallas. edu/mmm058000/reports/UTDCS-05-08. pdf)(2008).

[8] Zhao, David, et al. "Peer to peer botnet detection based on flow intervals." Information Security and Privacy Research (2012): 87-102.

[10] Al-Hammadi, Yousof, and Uwe Aickelin. "Behavioural correlation for detecting P2P bots." Future Networks, 2010. ICFN'10. Second International Conference on. IEEE, 2010.

[11] www.uvic.ca/engineering/ece/isot/datasets/

[12] http://malware.wikia.com/wiki/Sdbot

