Botnet Detection Framework

Punit Sharma
Research Scholar
CSE, AIET Jaipur
RTU, Kota (RAJ)

Sanjay Tiwari
Assistant Prof.
CSE, AIET Jaipur
RTU, Kota (RAJ)

Anchit Bijalwan
Assistant Prof.
Dept. of Computer Science
Uttarakhand Technical University

Emmanuel Pilli
Associate Prof. CSE, MNIT
Jaipur, (RAJ)

ABSTRACT

Botnet ia a collection on network of bots. i.e the collection of zombie computers which are controlled by a single person or group known as bot master or herder. This paper focuses on botnet detection framework and proposed a generic framework for botnet detection. The proposed framework is based on the approach of passively monitoring network traffic. This paer also show the flow chart of Generic Framework.

General Terms

Bot detection framework, bot analysis.

Keywords

Bot , network traffic, traffic flow .

1. INTRODUCTION

In the recent researches, One of the most serious & popular area of advanced malware is botnet. Bot is the small piece of code that can replicate itself. It takes command from the external sources..Botnet are the collection of large number of infected computers (bot)or zombie computers[1].Zombie are ordinary computer **attached** to the internet which are compromised by viruses, hackers, worm & Trojan horse. Such collection of infected computers are controlled by a single person or group, known as botmaster [2,3] or herder

We categorized this research paper in four section . In section two we covered the background , in section three the generic framework for botnet detection is proposed , section four discuss the analysis and tools .

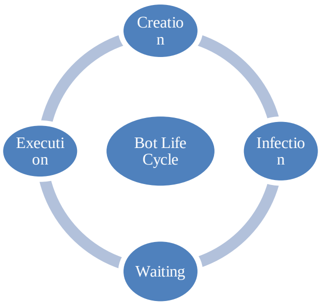

Fig.1 Bot life cycle

Schiller et al.[4] have specified the Life Cycle in Four phases**.**

Creation-This is a intial phase of botlife cycle in which the botmaster develop the malware software or some time botmaster use the existing software code. Infection-As the bot has been exploited, the life of botnet client begins. Bot can be exploited through a malicious code. Once a victim machine becomes compromised with a bot, It is known as Zombie. The possible vulnerabilities for infecting victim computer are Software Vulnerabilities, Unpatched vulnerabilities, Drive by download, Trojan horse, Email attachment, Phishing emails Spam Rallying. Waiting-In waiting phase botnet has joined with C&C network, which is concerned with its communication infrastructure & connectivity. Executing-After receiving the command from the botmaster bot execute it & returns the result to the botmaster via the C&C network. Commands given by the botmaster to bot are scanning for new victims, sending spam, sending DoS floods & setting up traffic redirection. After the execution of such command the bot returns to the waiting state for next instruction. If the victim computer lost its connection to the C&C network or rebooted, the bot resume in the rallying state.

Monitoring a machine or network with the aim of discover a specific kind of attack(bot),is known as botnet detection. Botnet detection technique is based on three approaches**.** Honeyne**t** Honeynet is used to understand the botnet technology & its characteristics. It is not mandatory that it detect bot infection. Honeypot. It situated on the network & closely monitored for infection. It gathers all about the malware operations like monitoring the botnet traffic & obtaining the Trojan payload. Passive network traffic monitoring and analysis: Botnet detection techniques based on passive traffic monitoring is useful to identify the presence of botnets.

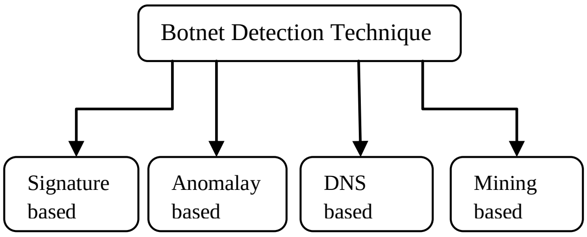

Fig. 2 Botnet detection techniques

Signature based-In this technique the knowledge of signature & behavior of existing botnet is required for the detection of botnet. The intrusion detection system(IDS) monitor network traffic in order to find sign of intrusion. Signature based detection technique is used for the detection of known botnet.

Anomaly based Detection-Anomaly based detection techniques is used to detect botnet on several network traffic anomalies such as high volume of traffic, high network latency, traffic of unusual ports & unusual system behavior that could show the availability of malicious bots in the network. **DNS-based Detection-** This technique is based on DNS information generated by a botnet.DNS based detection technique are all most similar to anomaly based detection technique as the similar anomaly algorithm are used on DNS traffic. **Mining based-Detection-**Botnet C&C traffic is difficult to detect. Anomaly based detection technique are not useful. Data mining techniques such as classification & clustering are used.

2. BACKGROUND STUDIES

Zeidanloo et al[5] proposed a new framework for botnet detection which is based on finding similar pattern communication & atleast one malicious activity performed among the group of hosts.The key point that distinguish there framework from other framework is that there is no need of prior knowledge of botnet signature.

Zeidanloo et al[6] proposed a new framework for botnet detection framework focused on P2P botnet.They proposed that bots performed correspondent communication & also perform the malicious activity within the same group of bots.They monitored the hosts with similar communication pattern in one step & performed malicious activity in another one ,also check the mutual host on them.

Chunyong et al[7] proposed a new P2P botnet detection framework which is based on tha alliance of common P2P network behaviours & host behaviours. Hailong et al [8]proposed a hierarchical collaborative model ,which distributes information & cooperates in the three stages of information ,features & decision making. They designed a botnet detection architecture based on collaboration. Their architecture is capable to extract mandatory features of botnet from various data.

SeungGoo et al[9] proposed a botnet framework for systematic detection & prevention. They also proposed a procedure & method for cooperation. Barthakur et al[10] proposed a proactive botnet direction framework applying Support Vector Machine(SVM) to analyze P2P botnet based on payload independent statistical features

3. GENERIC FRAMEWORK

The proposed framework is a generic framework of botnet detection which is based on the approach of passively monitoring network traffic. different network traffic & extract the exact behavior of particular. Our botnet detection framework focused on the traffic which generate from the network. We concentrate on the normal network traffic flow from the various tool such as PCAP , wire shark .

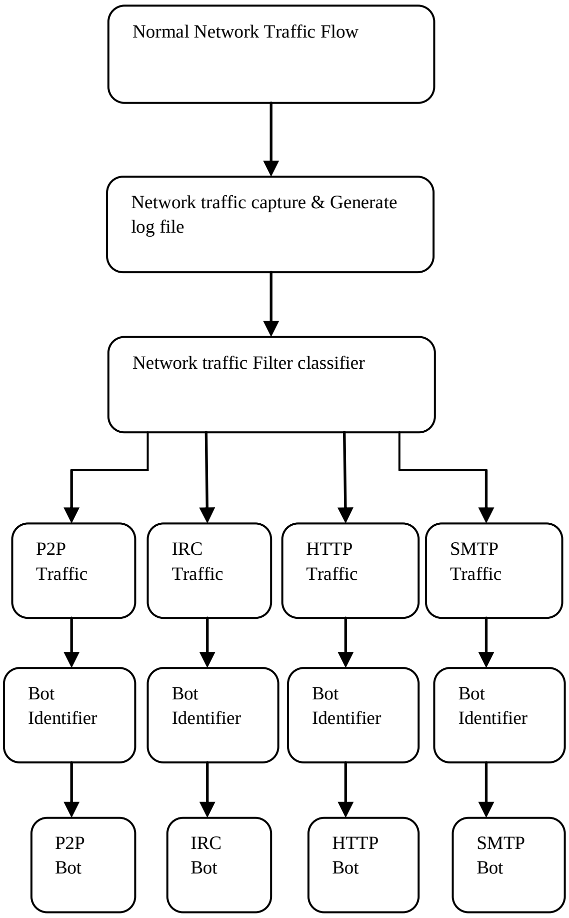

Fig.3 Generic Framework for botnet detection

We try to capture the network traffic and try to generate log files. After that we use the filtration process and use classifier on the among captured network traffic and the log files . We observed the different malicious activites, by the bot herder.

In P2P based network traffic, IRC based network traffic, Http based network traffic, SMTP based network traffic. Now our generic framework identified with its bot attack or it the different malicious attacks among P2P based network traffic,IRC based network traffic,Http based network traffic,SMTP based network traffic.Here we try to get P2P based bot, IRC based bot,HTTP based bot & SMTP based bot through bot identifier.Identifier used to find out the behavior of particular.

Traffic Monitoring:- Traffic monitoring is responsible is to detect different kind of similar behavior and pattern which help to observe phising activities by the black hat communities . Traffic monitoring continuously work in the network traffic. Network traffic monitoring captures the different network flow.

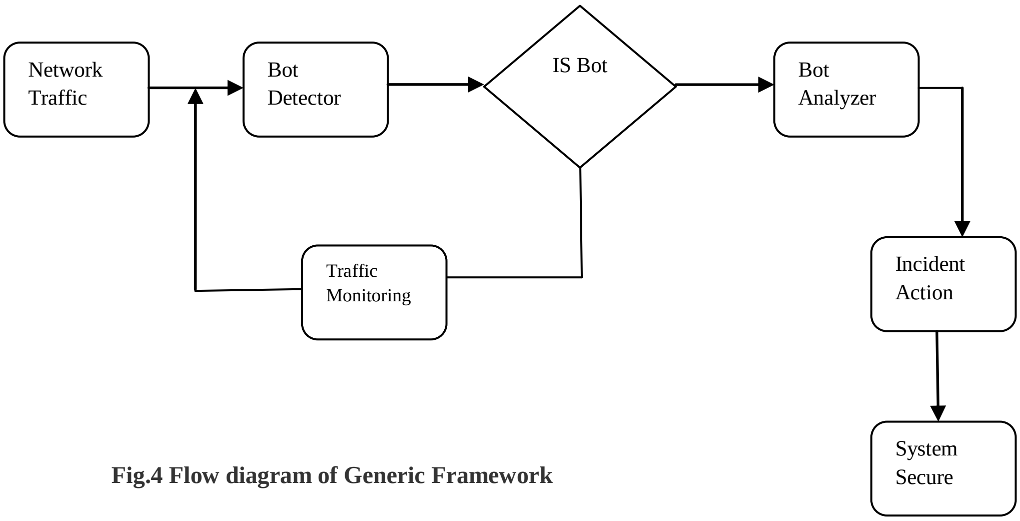

Fig.4 Flow diagram of Generic Framework

Bot Detector-Bot detector identifies the specific kind of malware which is known as bot through the network traffic.Bot detector identifies the clues fronm the record network flow & already captured the similar behavior from the traffic. If bot detector find any bot clues from the network traffic,forward it to the Analyzer otherwise the traffic monitoring continuously updated the network flow & record the same.

Bot Analyzer-Bot analyzer analyze the property of similar behavior & extract in to the various small similar patterns.Bot analyzer grouped to the bot into different similar activities.

Incident Action-In other word incident action & response is also known as Forensic investigation on bot.This is after crime investigation which is generally used after the crime happend.Incident action & response is a postmortem activity of botnet.It generally work on various stages such as collection,retention,observation & analysis.

System Secure-Postmortm treat & heal the malware through viruses away & maintain the system secure.All these steps make the system secure.

4. TOOLS AND ANALYSIS

Volatility-Volatility is one of the open forensic tool which is used to help the administrator to analyze what is going wrong in a system. It is implemented in python under the GNU (general public license).

Trident- Trident is also known as MSHTML . It is a application framework and software component written in C++. It allow the software developer to add web browsing functionality to their own application

Table-1 Description of Tools

S.No	Tool Name	Description	Machine	Phase
1	**Volatility**	Memory	Victim	Memory analysis
2	**TrIDnet**	Signature	Victim	Static analysis
3	**Wireshark**	Network	Destination	Dynamic
4	**TCP View**	TCP port	Destination	Dynamic

Wireshark- Wireshark is one of the most popular open source network protocol analyzer .Thisprotocol analyzer is used to captured the data in a network flow. It is a very powerful tool which provide network and upper layer protocol information about data captured in a network.

TCP- TCP view is a window program .It is used to analyze the all detail of TCP and UDP in the system observes the TCP & UDP end points .It It gives listing of all TCP and UDP endpoints including the local and remote address.

Table.2 Analysis of Tools in various phase

No.	Analysis phase name	Tool Name	Description	Contributions
1.	Static analysis	Dependency,Bin Text	Tools used to perform strings,specimen code relation	These tools provide detailed information about specimen
2.	Memory analysis	Nigilant32	Tools used to perform memory image	Real time memory image was performed with this tool
3.	Dynamic analysis	Wireshark,Cprts ,Procmom & Regmom	Tools used to monitor registry,files,ports &communication	Specific spybot behaviors were identified & evaluated with these tools
4.	Static code analysis	OllyDBG	Tools used to perform specimen code analysis	This debugger was used to identify code subroutines
5.	Dynamic code analysis	IDA-PRO	Tools used to perform dynamic specimen code analysis	This tool was used to perform specimen code analysis

5. CONCLUSION

Botnet detection system has the ability to detect unknown botnets which are independent of their C&C protocols. These are some network based methods which does not rely on packet contents for faster processing and privacy issues. To adopt mitigation efforts ,detection should be in real time. There should be low false positives to detect botnet activity as in intrusion detection system. Evade detection should be considered as one of the most important features for attackers.

In general, current , against bot net current mitigation efforts are similar to mitigation of malware, intrusion cyber crime. In mitigation efforts , to include bonnets , botnet analysis and detection system feed existing solutions.

In enterprise network , bot detection constitutes cleaning of infected hosts. It is essential to find the IP addresses of C&C servers because firewalls with blacklists can block the communication with C&C servers. So ports(eg. IRC PORT 6667) , protocols(eg.IRC) and hosts(infected hosts or C&C servers) can be blocked. C&C channel will be broken and corresponding ports will become useless. For C&C, if HTTP and custom protocols are used than the task is much more difficult. Deep Packet Inspection(DIP) is required to filter the web traffic based on the packet content and can not be blocked.

6. REFERENCES

[1] Ming Yang, Gang Ren, Jianwei Zhang, “ Talk about botnets”. The community communications conference 2006:629-633.

[2] A. Ramachandran, N. Feamster, and D. Dagon, "Detecting botnet membership with dnsbl counterintelligence," *Botnet Detection*, pp. 131-142, 2008.

[3] E. Cooke, F. Jahanian, and D. McPherson, "The zombie roundup: Understanding, detecting, and disrupting botnets," in *Proceedings of the USENIX SRUTI Workshop*, 2005, p. 44.

[4] C. Schiller and J. R. Binkley, *Botnets: The killer web applications*: Syngress, 2011.

[5] Zeidanloo, Hossein Rouhani, A. Bt Manaf, Payam Vahdani, Farzaneh Tabatabaei and Mazdak Zamani. 2010. "Botnet detection based on traffic monitoring." In Networking and Information Technology (ICNIT), 2010 International Conference on: IEEE.

[6] Zeidanloo, Hossein Rouhani, Azizah Bt Abdul Manaf, Rabiah Bt Ahmad, Mazdak Zamani and Saman Shojae Chaeikar. "A proposed framework for P2P Botnet detection." IACSIT Int. J. Eng. Technol 2:161-168.

[7] Yin, Chunyong and Ali A. Ghorbani. 2011. "P2P botnet detection based on association between common network behaviors and host behaviors." In Multimedia Technology (ICMT), 2011 International Conference on: IEEE

[8] Hailong, Wang and Gong Zhenghu. "Heterogeneous Multi-sensor Information Fusion Model for Botnet Detection." In Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on: IEEE.

[9] Ji, SeungGoo, ChaeTae Im, MiJoo Kim and HyunCheol Jeong. 2008. "Botnet detection and response architecture for offering secure internet services." In Security Technology, 2008. SECTECH'08. International Conference on: IEEE.

[10] Barthakur, Pijush, Manoj Dahal and Mrinal Kanti Ghose. 2012. "A Framework for P2P Botnet Detection Using SVM." In Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012 International Conference on: IEEE