International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 1, ISSN No. 2455-2143, Pages 108-112
Published Online November-December 2016 in IJEAST (http://www.ijeast.com)

BOTNET ANALYSIS & DETECTION

Varidhi Garg
Department of CSE
M.A.I.T, Delhi, India

Srishti Garg
Department of CS
University of Delhi, Delhi, India

Abstract— Recent developments of remote services in distributed computing environment have led to growth of various threats related to internet security and user privacy. One of the prominent threat that is gaining pace is the Botnet phenomenon, which exploits these services for malicious purposes. Botnet is a collection of various Bots, where each one of them perform a predefined set of functions in automated fashion. The botnet supports a wide range of attacks including phishing, Distributed Denial of Service (DDoS) attacks, spamming, illegal exchange of information, and many more. This paper presents a brief review of botnet and related researches including its types, life cycle, communication protocols, detection systems and mitigation mechanisms available.

Keywords— Botnet, Botnet mitigation, Botnet detection

I. INTRODUCTION

Evolution of distributed computing models have eventually led to evolution of various malicious software. Earlier these attacks had a local impact and was limited to small scale only but due to widespread use of internet technologies, these can attack millions of systems around the world. Botnet is one of the serious threat that occurs to cyber security and is gaining popularity these days. The term Bot is a generic term to describe a script or program that perform a predefined function in an automated fashion. Collection of such bots is called a Botnet. Generally, network of systems compromised by these bots may is referred as Botnet. A Botmaster[1] is present which controls these infected systems. A Botnet consists of a Control and Command(C&C)[1] infrastructure between the botmaster and infected system, which provides a specific channel for communication which can operate over a variety of topologies and use established internet protocols.

In general, main difference between Botnet and other kinds of malware is the existence of C&C infrastructure[6]. Botnet detection systems locate these infrastructures and disable them to remove and prevent the attacks caused by them. But it also depends on the protocols used by Botnet to perform these attacks.

On the other hand, botnet are capable performing various ethical tasks. Google search uses google bot[2] to search any information from the websites and its database, games use bots as virtual opponents, IRC bots are used to supervise IRC channels and other such useful activities.

II. BOTNET PHENOMENON

Botnet is an attractive tool for cyber criminals and pose a great threat against cyber security. Most of them use distributed computing platforms predominantly for illegal activities such as triggering DDoS attacks, sending phishing mails, spamming, stealing information, click fraud, etc.

A. *Characteristics*

Botnets have following features through which they are uniquely identified from other types of malwares:

- Bots are usually small script or program that perform a specific function by taking commands from botmaster.
- They are self-propagating applications that infects vulnerable hosts.
- Defining characteristic of botnet is the use of C&C channels through it can be updated and directed. Many botnets are classified on the basis of C&C architecture.
- Purpose of botnet is not always unethical. Their capabilities are exploited in a bad fashion to use it for such purpose.
-

B. *Lifecycle of botnet*

Botnet phenomenon follows a general flow or life cycle. It follows certain steps to become active. The initial phase starts with setting up of various parameters to initiate a connection. Static IP address is allocated to botmaster using DDNS. After initial phase, the usual process of propagation of bots occurs in various forms, for example, by infected storage devices, sending malicious content via email, unwanted downloads, etc. Each bots gets added to bot network as soon as it gets executed by establishing connection with botmaster, a process also known as rallying[2]. It involves setting up of connection between bots and their C&C, to ensure continuous connection between them and able to receive commands for taking actions. Next step involves the execution of malicious activities including DDoS attacks, propagation of malware, access private files and documents, pilfering network resources, etc. Final stage of lifecycle includes maintenance of botnet and its upgradation. Maintenance includes maintaining proper communication and coordination between bots. Also, upgradation is required to update binary code for the bot army for handling various detection techniques and adding new features.

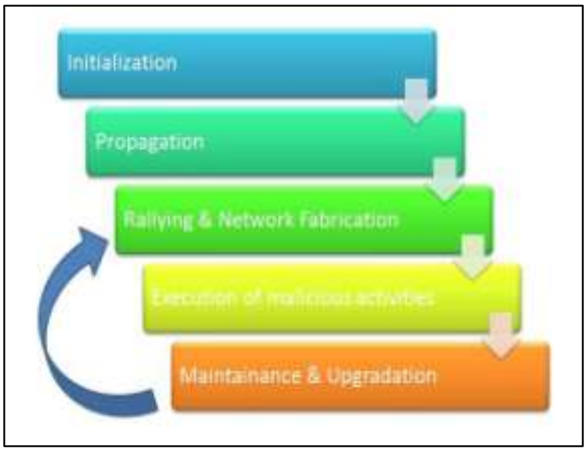
Initialization
Propagation
Rallying & Network Fabrication
Execution of malicious activities
Maintainance & Upgradation

Fig. 1 Lifecycle of botnet

C. *Botnet Architectures*

According to C&C channels, we can categorize botnet topologies into three different types of models[1][2], which are discussed below:

i. **Centralized model**

It views the network as a typical star topology where C&C server is the central point and bots (including botmaster) are connected to it for exchanging commands and data between them. Advantage of this model is the presence of direct connection to central point or C&C server which leads to low latency for communication. But same central point act as weak point for this botnet, because if it goes non-functional then complete network will not work, and hence its disadvantage.

ii. **Decentralized model**

Here the idea of Peer-to-Peer communication as a Command and Control pattern which is less susceptible to failure as in the centralized model. Bots act as both client and server in this model, therefore there is no centralized point for communication. Each keeps connection to other bots in the network. In this model the communication system does not completely depend on some selected server.

iii. **Hybrid model**

It includes both the features of centralized and decentralized model. Bots are classified into servant and client bots, where servants act as both client and server with static IP address and client is configured using dynamic IP address for listening incoming connections.

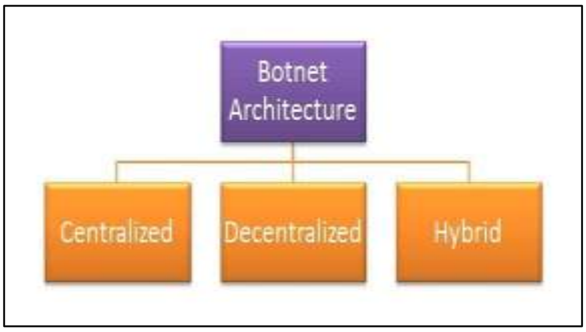

Fig. 3 Types of Botnet Architecture

III. BOTNET DETECTION

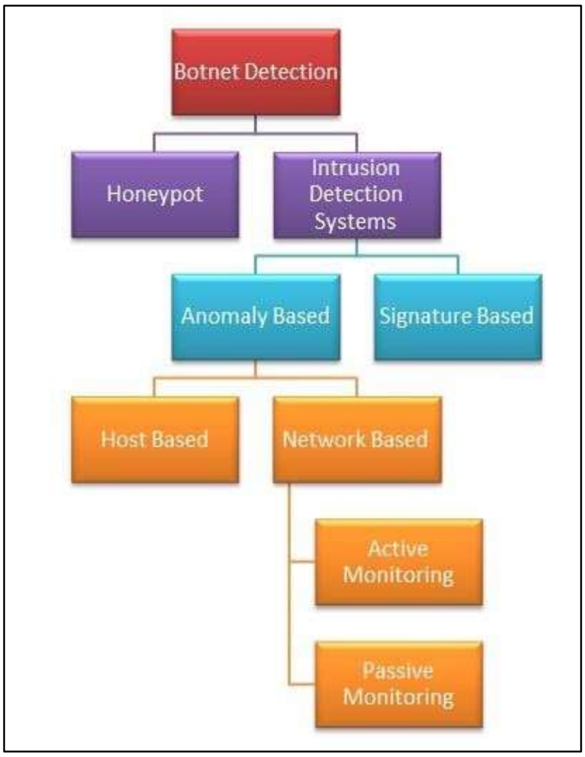

Fig. 2 Hierarchy of Botnet Detection Techniques

Detection of botnets is becoming popular topic these days due to increase in malicious activities. Although detection can be a difficult task but it is not impossible also. There exist various types of botnet and most of them require different techniques to handle them. For e.g. some botnets can be detected using analogy based methods while others require a dynamic method that adapts to evolved version of botnet. Botnet detection techniques are classified into two broad categories:

A. Honeynet based method

A honeynet[1][2] mainly consists of two parts: honeybot[2] and honeywall[2], which are used to collect and analyze activity of bots in a network. Honeypot is an end host that is easily vulnerable to a malicious attack whereas the honeywall denotes a utility that which is used to monitor, collect, control and modify the traffic. A honeynet is also used to detect bot-binaries which try to penetrate into botnet. Various techniques are used to detect bots using honeynets to detect malicious attacks. But as the botnets are getting advanced and dynamic, they are able to surpass these detection systems. Main advantage of honeynet based method is the simplicity to deployment with low cost, less resources are required and compatibility to IPv6 environments. Apart from vantage, botnets come with some critical aspects such as:

- Limited scale deployment
- Discovery of infected system as trap is difficult
- As honeynet are easy to compromise, they can easily be exploited to harm themselves or other systems in honeynet network

B. Intrusion Detection Systems

Monitoring is done using an Intrusion Detection System (IDS)[2], which is a software application or hardware to monitor system services for unusual activities or anomalies. If some policy is violated, the IDS reported to the management system for necessary actions to mitigate. It is further classified into two categories as a signature based approach and anomaly based approach[2]. Main advantage of IDS is the implementation of repository to collect signatures of various known botnets for use in future detection but frequent updating is required for such knowledge base repository for detecting newly activated botnets. Due to rapid increase in anomalies, refresh rate for signatures is slow and therefore the detection is not too fast. Anomaly based techniques monitors the abnormal behavior of host to detect the activities of malwares. In order to do so, the system is trained to detect activities which do not follow normal behavior. It is different from signature based approach in which the only attacks for which previous signatures are present can be detected. System can be taught to do so by data mining techniques by analyzing the traffic or using the artificial intelligence type techniques. Anomaly based techniques do have some short comings such as high false positive rate or misinterpretation of a correctly delivered attack.

Further Anomaly based techniques are classified into two categories based upon method of detection of anomalies, it can be either done by collecting information about activity on a particular system or host, known as host based techniques or collecting information from the network itself rather than separate systems, known as network based techniques.

i. **Host Based Techniques**

It is specifically based on the detecting certain type of anomalies in the host/system. The system under monitoring is compared with a system functioning normally i.e. system which we know is not a part of botnet. The host based detection technique unravels only the infected host not the bot herder or C&C server which only secures a particular host and not disrupts the whole botnet. In host based detection anomalies like rootkit detection[2] packages, host file modification, random click-fraud activity and machine slowness are examined. The entirety of host based detection system is the analysis of the system state and contents which includes its host file, DNS records, memory contents and process permissions, also some special memory regions which should not have been modified. The host based detection system checks for the anomalies of the host, which generally may go unnoticed by the network based detection system as the dynamic bots are smart enough to manipulate traffic packets and C&C server may change its IP address periodically. The HIDS[2] creates a database of newly detected bots which is used to detect same type of bots by comparing the checksum of files and searching it in the database.

ii. Network Based Techniques

Information is collected from the data that travels in a network. Headers and contents of all the packets that are circulating in the network are inspected. Network sensors[2] detect the attack by comparing it with the attack signatures which includes various parameters such as traffic behavior, traffic patterns, network load, response delay, etc. and allow identifying hostile traffic. Most of these systems are portable and independent of the operating systems that they are installed on which makes it convenient to deploy with lesser cost and effort. Also, they are beneficial where network topology remains inconsistent or system resources need to be moved. It can also be classified further into two categories of botnet detection using network based techniques i.e. active and passive monitoring[7], depending upon the way the network traffic is analyzed.

Active Monitoring[2] uses new packets for injecting into the network to detect malicious activities in it. It increases load in network traffic. Sometimes, it can get difficult to differentiate normal traffic from artificially created traffic which disrupts the routine traffic. Passive monitoring[2] is another scheme used in this type detection method in which instead of creating new packets for detection, the current data stream is analyzed through the communication medium. Therefore, no additional load is required and hence its performance is better than the active method discussed above. According to protocol used for e.g. SMTP, P2P, HTTP and DNS, passive monitoring methods are divided into subcategories. Similarly, they are categorized on the basis of their application models used also. Some of them are described in brief below:

- Machine Learning: Detection based on machine learning has been a subject of interest of research community, which resulted into various detection based methods that target various botnets using diverse machine learning algorithms. This class of detection presents a strong ability to detect botnet traffic and could be improved further by increasing its efficiency, ability to adapt and performance.

- Data mining: Non trivial extraction of implicit, previously unknown, and potentially useful information from data is called data mining[4]. Methods such as statistical data analysis, pattern recognition, artificial neural networks, support vector machines, etc. are used in detection schemes. Main goal of this technique is to provide a mechanism for detection of new classes and variants of bots.

- Graph Theory: It provides a model which can be used to visualize logical relationship between the objects or entities. Therefore it is easy to identify and isolate malicious nodes from the network using various algorithms[5]. A distributed computing environment is preferred for such graph theory based detection systems to decompose graph construction and computation in parallel to increase the efficiency of the same.

- Web based: It is hard to identify and locate such type of attacks where communication traffic of bots is included in normal traffic of internet of a user. Therefore, HTTP botnet[3] attacks are serious threat because it takes advantage of HTTP connections where malicious traffic is enclosed in huge amount of standard traffic but the communication pattern of botnets remains the same with difference in some parameters, so present detection types can be further evolved to detect these types of botnets.

- DNS based: Bots also produce DNS traffic to carry out DNS queries in a network. This particular traffic can be captured and analyzed for anomalies to locate the server of the botnet.

DNS queries can provide information regarding botnet existence and help to find C&C server localities. Normally, bots communicate within a single domain and by analyzing different domains such as TTL of query, frequency, etc.[2].

IV. CONCLUSION

Botnet pose a significant and growing threat against cyber security. It provides a key platform for many cybercrimes around the world. As the network security has become integral part of our life and botnets have become serious threat to it. So it becomes crucial to find a solution to detect botnets. Therefore, Botnet detection is an important part of network security as no network is secure with bots nesting among its hosts. Nowadays , due to dynamic nature of botnet which can update their bots regularly, it is not sufficient to monitor the host as updated bot will require a new detection technique, so a network based detection is an alternate solution. The network based detection of botnet is neither superior nor inferior to host based detection but network based detection allows us to find the patterns on which common botnets work. Network based detection along with host based detection can eliminate the botnet presence from a network. The fact that we can recognize and eliminate C&C server and bot herder from a botnet using network based detection puts this type of technique in front of others as without C&C server bots cannot take and execute commands from their herder. Hence a dynamic approach is desirable using a flexible and structured architecture, to detect botnets because it delivers a method to detect various types of botnets based on previous signatures or evolving botnets with different signatures, at the same time. This will allows for the integration of wide ranging techniques and therefore not limiting the architecture to support only a single type or class of detection algorithms.

V. REFERENCES

[1] Amit Kumar Tyagi and G. Aghila, “A Wide Scale Survey on Botnet”, International Journal of Computer Applications, Volume 34– No.9, November 2011

[2] Ahmad KARIM, Rosli Bin SALLEH, Muhammad SHIRAZ, Syed Adeel Ali SHAH, Irfan AWAN, and Nor Badrul ANUAR, “Botnet detection techniques: review, future trends and issues”, Journal of Zhejiang UniversitySCIENCE C (Computers & Electronics), January 2014

[3] Chen, C.-M. And M.-Z. Huang, “Detecting

Web-Based Botnets with Fast-Flux Domains", Advances in Intelligent Systems and Applications-Volume 2, Springer: p. 79-89, 2013

[4] Robert F. Erbacher, Adele Cutler, Pranab Banerjee, and Jim Marshall, "A Multi-Layered Approach to Botnet Detection", Utah University

[5] Yao Zhaoy, Yinglian Xie, Fang Yu, Qifa Ke, Yuan Yu, Yan Cheny, and Eliot Gillum," BotGraph: Large Scale Spamming Botnet Detection", Northwestern University, Microsoft Research Silicon Valley, Microsoft Corporation

[6] Ravi Kishore Sharma and Gajendra Singh Chandel, "Botnet detection and resolution challenges: a survey paper ", International Journal of Computer, Information Technology & Bioinformatics (IJCITB) ISSN: Volume-1, Issue-1

[7] "Host vs. Network-Based Intrusion Detection Systems", Global Information Assurance Certification Paper

[8] Guofei Gu, Junjie Zhang, and Wenke Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic", Georgia Institute of Technology

[9] Ping Wang, Sherri Sparks, and Cliff C. Zou, "An Advanced Hybrid Peer-to-Peer Botnet", School of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL

[10] Plohmann, D. and E. Gerhards-Padilla, "Botnets: Detection, measurement, disinfection & defence." The European Network and Information Security Agency, 2011