Survey on Botnet

Darshana Soni[1], **Jignesh Vania**[2]
[1]Pursuing Master, [2]Faculty
[1,2]Department of Computer Science and Engineering
[1,2]L.J.I.E.T., Ahmedabad, India

Abstract— Now days internet users are increased drastically, with those malicious activities through internet have also been increased. One of the most commonly occurring and serious attack is botnet. Botnet is group of compromised computers and they are controlled remotely by the botmaster. And further more hackers also have started using fluxing techniques to evade the detection. It is impossible to detect and stop them completely. Here in this paper we discuss botnet in detail with its characteristics and some of its attacks and detection techniques.

Key words: bot, botnet, botmaster, C&C, attacks, detection

I. Introduction

Botnets are one of the biggest threats in this internet technology. It is used for the malicious activities like attacks, hack the servers, stealing sensitive information and committing fraud. A study shows that, on a typical day, about 40% of the 800 million computers connected to the Internet in a botnet[1].

Botnets are the collection of computers which are under control of some hacker. Some kind of software those computers are installed with user intimation and are remotely controlled called 'bot'. These computers are being controlled by via the command and control server.

An active Botnet initializes its attack by first exploiting vulnerabilities in the user computers. It then downloads the malicious binary and executes it locally. This program logs on to the Command and Control Server (C & C) and notifies its Host, commonly known as „Botmaster‟ or „Botherder‟, that the computer is now converted to a „Bot‟. It can now be used to forward its affect to other computers by repeating the same procedure[2]. This process can be done by continuously communicating with the bots. It can be done by different networks like centralized and decentralized. This is the main difference between the botnet and other threats.

II. Botnet characteristics

Botnets are emerging as the most significant threat which is used to perform cyber crime attack to steal the valuable data of users that is we can say Botnet perform attack after facing online ecosystems and computing assets[10].

Among the other malwares, the main characteristic of botnet is that is using the C&C mechanism through which systems are directed and they are updated if required. This characteristic of Botnet provides anonymity for the Botmaster. Using C&C channels the botmaster can operate a wide range of different network topologies and different protocols.

Botnet can be classified as

- IRC based,
- HTTP based,
- P2P based.

The IRC user usually creates a group on MIRC messenger and invites users of some specific interest[11]. Administrator of the group first provides them whatever they want and then makes them to accept the malicious code. Then whenever users connect to internet they are ready to attack on specific server or application. HTTP protocol is a popular Botnet due to its communication method by sending message as HTTP response and HTTP GET response to perform attack which is difficult to be detected. So Using the HTTP protocol, Botnet usually bypass security devices[10]. Recently, P2P based botnet is used[1]. This protocol is used to avoid the single point of failure. These kinds of botnets are hard to detect, shutdown or hijack.

III. Botnet architecture

Botnet uses four types of architectures to manage the networks and to evade from detection.

- Centralized (IRC based) Architecture,
- Decentralized (Peer to peer) Architecture,
- Hybrid Architecture.

A. *Centralized (IRC based) Architecture*

It is the oldest and easiest architecture to manage and control the network. In this type of architecture all the compromised computers are connected to a single point. It is easy to detect and stop.

This type of architecture uses the IRC and HTTP protocol for its command and control server. Advantage of this model is small message latency which cause Botmaster easily arranges Botnet and launch attacks[10]. Figure 1 demonstrates this architecture.

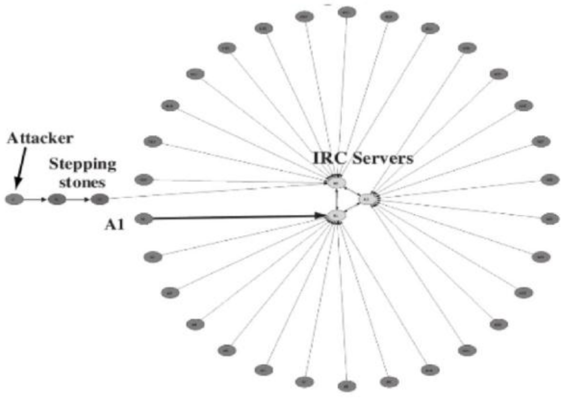

Fig. 1: Centralized Architecture(source: [7])

B. *Decentralized Architecture*

As the centralized architecture is having the drawback of *single point failure*, hackers start using decentralized approach. They decided to find a model in which the communication system does not heavily depending on few selected servers and even discovering and destroying a number of Bots[7].It is hard to detect and destroy.

In decentralized approach hackers start using HTTP as well as P2P protocols. Supervisor-bot transfer command to an infected zombie peer[10] who transfers it to other peers, acting both as Supervisor- bot and zombie army soldier[11].

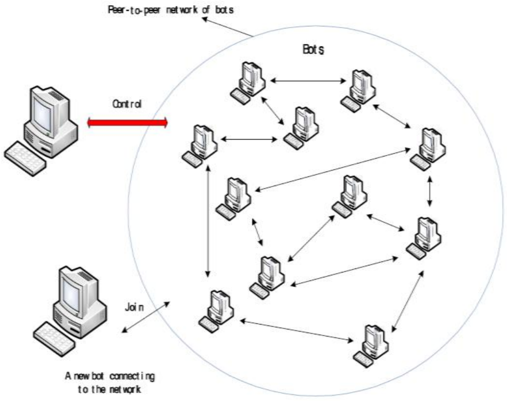
Peer-to-peer network of bots
Bots
Control
Join
A new bot connecting to the network

Fig. 2: Decentralized Botnet Architecture

As shown in the figure 2, in decentralized architecture there is no any central point to communicate. Each and every bot is connected to the other bots in the botnet. Each bot in this type of architecture works as both client as well as server. A bot must know the addresses of network to connect so in such architecture if any bot is offline the botnet can still be operated by the Botmaster.

C. *Hybrid Architecture*

In this type of architecture bots are act in two different groups:

1) *Servant Bots:*

Bots in this group are working as both Client and server. They are having both static as well as routable IP addresses. They can be accessed from entire internet.

2) *Client Bots:*

They do not accept incoming connections. This group contain different types of bots

- Bots with Dynamic designed IP addresses,
- Bots with NON-routable IP addresses,
- Bots behind firewalls. They cannot be connected to global internet.

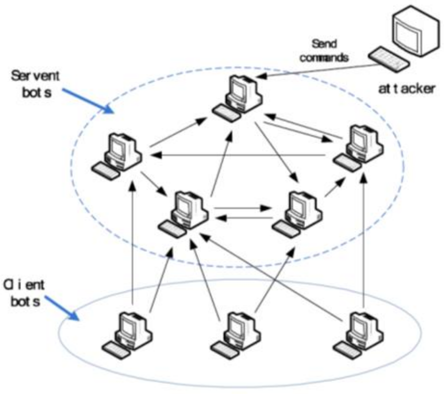

Fig. 3: Hybrid Architecture

IV. BOTNET LIFE CYCLE

Work of Botnet is distributed in different into five phases:

- Phase of spread
- Phase of Infection
- Phase of Control
- Phase of Attack
- Phase of Destruction

A. *Phase of spread:*

An attacker of the botnet must gather number of victims to acquire some goals to attack. For that attacker makes numerous bots and spread them to the computers who are infected. These infected machines will also spread these bots.

B. *Phase of Infection:*

Once a computer has downloaded or installed the bot, it will be executed automatically to infect the whole system. During this phase the victim machine will join the command and control channel.

C. *Phase Of Control:*

A victim machine will acquire the commands from the C&C channel. It functions differently in different protocols' environments.

D. *Phase Of Attack:*

Attackers now use the botnets to initiates different attacks to target some websites or to send large number of spams.

E. *Phase Of Destruction:*

After performing malicious activities for better protection sometimes botmasters destruct part of botnets.

V. BOTNET ATTACKS

A Botnet can be said as a tool for users who wants to perform attacks. Using Botnet for malicious activities can be beneficial for the hackers as they provide evade of detection. Most used of the botnets is for destructive purpose or to steal the valuable information. Here are some Botnet attacks which are detected till now:

- DDoS (Distributed Denial of Service) attack
- Spamming
- Spread new malwares
- Click fraud
- Google AdSense abuse
- Attacking IRC networks
- Fast Flux
- Sniffing Traffic
- Key Logging
- Mass identity theft

A. *DDoS attack:*

It is an attack on a network that causes a loss of network connectivity and services, by consuming the bandwidth of the user's network or high bandwidth or overloading the computational resources of the user's system.

B. *Spamming:*

It is an attack which is performed by sending malicious links to user through internet.

C. Spread New Malwares:

Botnet is used to spread the malwares and it is easy because all bots implement such mechanisms to download and execute a file via HTTP or FTP.

D. Click Fraud:

It is an internet crime that occurs on clicking on some online advertisements. When a person click on the link automated script generates a fake user of a web browser.

E. Google Adsense Abuse:

In this attack, attacker offers companies the possibility to display Google advertisements on their own website and earn money this way. The company earns money due to clicks on these ads.

F. Attacking IRC Networks:

In this attack, victim network is over flowed by service requests from thousands of bots. Through which the victim IRC network is crashed.

G. Fast Flux:

This is a service network in which networks of compromised computer systems with public DNS records that are constantly changing, for short time to perform illegal content from the Botnet end point to a central server. So the main aim of this technique is to provide high availability of the malicious contents by hiding location of the main hacker.

H. Sniffing Traffic:

By using the sensitive information like usernames and passwords, this attack is done. In which Bots can also use a packet sniffer to watch for interesting clear-text or data passing by a compromised machine.

I. Key Logging:

It is the action of tracking the keys pressed on a keyboard in a hidden manner. The person using the keyboard is unaware that their actions are being monitored and traced by an attacker. Through this attack, it is very easy for an attacker to retrieve sensitive information.

J. Mass Identity Theft:

This is the one of the fastest growing crimes on the Internet to identity theft. Bogus emails ("phishing mails") that pretend to be original ask their intended victims to go online and submit their private information. These fake emails are generated and sent by bots via their spamming mechanism to perform an illegal activity.

VI. DIFFERENT DETECTION TECHNIQUES

Detection of Botnet and to trace it has been a serious and major research topic in recent years. For these, different solutions have also been proposed. There are mainly two approaches for detection and tracking. One approach is based on setting up honeynets which can be considered as an active analysis[12].The second approach is based on passive network monitoring and analysis it can be classified as signature-based, DNS-based, anomaly-based and mining-based. These approaches are explained as following.

A. Honeypots and honeynets:

We can define honeypot as an "environment here vulnerabilities have been intentionally introduced to observe attacks"

They have a strong ability to detect security threats, to collect malware signatures and to understand the motivation and technique behind the threat used by hacker. In a large network, different size of honeypots creates honeynet. Generally, honeynets based on Linux operating systems are preferred.

Honeypots are classified as high-interaction and low-interaction according to their emulation capacity [12]. A high-interaction honeypot can copy almost all aspects of a real operating system. It gives responses for known ports and protocols as in a real zombie computer. They allow intruders to gain full control to the operating system. On the other hand, low-interaction honeypots copy only important features of a real operating system and they do not allow full control to the operating system.

As honeypots and honeynets are very popular in detecting threats, hackers are in searching of new ways of protecting honeypot traces. Some feasible techniques are used by intruders like emulator virtual machines, detecting incoherent responses from bots.

B. Signature Based Detection Techniques:

In this type of detection knowledge of useful signatures and behavior of existing botnets is required for detection. For example, Snort is an open source intrusion detection system that monitors network traffic to find signs of intrusion[4]. However signature-based detection techniques can be used for detection of known botnets. Thus, this solution is not useful for unknown bots.

C. Anomaly Based Detection Techniques:

Anomaly based detection has high false positive rate due to complication involved in determining, the features to be brought under considerations. These techniques get signals of availability of bots by the different characteristics like high volumes of traffic, traffic on unusual ports, and unusual system behavior in the network [11]. Anomaly based detection cannot detect a botnet in sleep mode unless it is being awaked and start using. But Binkley and Singh solved it by combining TCP based anomaly with IRC tokenization and IRC message statistics to create a system which can detect client and server BOTNETs if IRC commands are not encrypted [11].

D. DNS Based Detection Techniques:

DNS-based detection techniques are based on particular DNS information generated by a botnet. These techniques are similar to anomaly detection techniques as similar anomaly detection algorithms are applied on DNS traffic. Bots typically initiate connection with C&C server to get commands. In order to access the C&C server bots perform DNS queries for locating the respective C&C server that is typically hosted by a DDNS provider. Thus, it is possible to detect botnet DNS traffic by DNS monitoring and detect DNS traffic anomalies.

E. Data Mining Based Detection Techniques:

Anomaly based techniques are mostly based on network behavior anomalies. However C&C traffic usually does not reveal anomalous behavior. It is mostly hard to differentiate C&C traffic from usual traffic behavior. At this point pattern recognition and machine learning based data mining techniques are very useful to extract unexpected network patterns. Firstly it can be useful to introduce a research of preprocessing tasks of anomaly and data mining based botnet detection systems[11]. Researcher introduce a review of known preprocessing tasks for anomaly based and mining based intrusion detection techniques.

VII. CONCLUSION

By this survey paper reader can get deep understanding of the botnet. It is analyzed that it is impossible to stop and detect the botnet threats completely. As botnet is widespread it is hard to detect and stop from spreading. Our main aim is to increase the awareness in creating the different and efficient models.

REFERENCES

[1] Chao Li, Wei Jiang, Xin Zou, "Botnet: Survey and case study", 2009 Fourth International Conference on Innovative Computing, Information and Control,2009 IEEE.

[2] Fatima Naseem, Mariam shafaqat, Umbreen Sabir, Asim Shahzad, "A survey of Botnet Technology and Detection", International Journal of Video &Image Processing and Network Security IJVIPNS-IJENS Vol:10 No:01,2010.

[3] Haritha.S.Nair, Vinodh Ewards S E,"A study on Botnet Detection Techniques", International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012.

[4] Maryam Feily, Alireza Shahrestani, "A survey of Botnet and Botnet Detection", 2009 Third International Conference on Emerging Security Information, Systems and Technologies.

[5] Lei Zhang, Shui Yu, Di Wu, Paul Watters, "A Survey on Latest Botnet Attacks and Defense", 2011 International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11.

[6] Dae-il Jang, Minsoo Kim, Hyun-chul Jung, Bong-Nam Noh, "Analysis of HTTP2P Botnet: Case Study Waledac", Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications, 15-17 December 2009 Kuala Lumpur Malaysia.

[7] Hossein Rouhani Zeidanloo, Azizah Abdul Manaf, "Botnet Command and Control Mechanisms", 2009 Second International Conference on Computer and Electrical Engineering.

[8] Meisam Eslani, H. Hashmi, N.M. Tahir, "AN Efficient False Alarm Reduction Approach in HTTP based Botnet Detection",2013 IEEE Symposium on Computers & Informatics,978-1-4799-0210-1/13/$31.00 ©2013 IEEE.

[9] Lei Cao, Xiaofeng Qiu, "Defence Against Botnets: A Formal Definition and a General Framework", 2013 IEEE Eighth International Conference on Networking, Architecture and Storage.

[10] Amit kumar tyagi, G.Agila, "A Wide Scale Survey on Botnet", International Journal of Coputer Applications(0975-8887), Volume 34- No.9, November 2011.

[11] Ihsan Ullah, Naveed Khan, Hatim A. Aboalsamh, "SURVEY ON BOTNET: ITS ARCHITECTURE, DETECTION, PREVENTION AND MITIGATION", 978-1-4673-5200-0/13/$31.00 ©2013 IEEE.

[12] Erdem Alparslan, Adem Karahoca, Dilek Karahoca, "InTech Botnet _detection_enhancing_analysis_by_using_data_mining_techniques", http://dx.doi.org/1