A Survey on Botnet Analysis and Detection

Divyang Rahevar[1] Mr. H. P. Sanghvi[2]
[1]Student [2]Asst. Director
[1]Institute of Forensic Science Gujarat Forensic Sciences University Gujarat, India
[2]Directorate of Forensic Science, Gandhinagar, Gujarat

Abstract---Botnets are the network of the computers that are compromised and controlled by the Botmaster or an attacker. Botnets are used for the spamming, phishing, stealing private information, click fraud and Distributed Denial of Service (DDoS) attack on computer networks. Different types of Botnets are used for the different purposes. The number of new Botnets in the network creates the challenge for the AV companies to detect them. This paper focuses on different types of Botnets and analysis and detection techniques.

Keywords: Botnet, DDoS Attack, Malware, Spam, P2P Botnet.

I. INTRODUCTION

As the use of Internet is increasing the activity of cyber criminals is also growing parallel. The cyber-attacks can generate the revenue so it is the interesting area for the attackers for making money on fingers. Botnet which is the network of compromised computers are used for Email spamming, click fraud, DOS and DDoS attacks. Botnets are used to attack the target at the same time which is controlled by Botmaster [1]. The aim of the Botnet based DDoS attack is to block the available resources to their users.

A software program that controls the computers for specific task is called "bots", are small scripts designed for automated functions [2]. The bots are categorised by their use of a command & control (C&C) channel. Using this C&C channel the attacker can take advantage of the zombie machines for performing the attack. This bots are used for stealing the personal information, stealing bandwidth, spamming and performing DDoS attack. The topologies used by the botmaster are star; Multiserver, Hierarchical and Random using C&C channel [3].

II. CHARACTERISTIC AND ARCHITECTURE OF BOTNET

There are different types of Botnets according to the type of the attack the different types of bots are used. The early Bots were setup on the public chat servers but now the Botmasters are putting it to the private chat server.
The characteristic of the Botnet is described as below points.

- It can run on victim's computer.
- Connect back to the Botmaster.
- It can receive and respond to the commands of the Botmaster.
- Main point: Deployed without the knowledge of the user.

The Botnet uses mainly three types of command & Control architecture they are: Centralized, P2P and Unstructured.

A. Centralised Architecture: The centralised architecture of the Botnet uses the standard client-server architecture. This architecture uses IRC protocol for control and a centralised communication of the bots. In centralised architecture the botmaster has created the bots. The bots are connected to the botmaster via the command and control channel server. The botmaster gives the command to the bots for performing an attack to a particular host or server. The figure shows the centralised architecture of the Botnet.

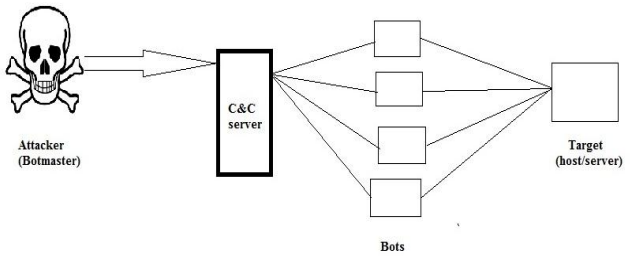

Fig. 1: Centralized architecture

In the given figure the small rectangular boxes describe the host infected by the bots. Which are given the command by the attacker through C&C server to attack on target host at a particular time?

B. Peer to Peer Architecture: in the P2P architecture some hosts are under the control of the botmaster. The botmaster gives command to this host and the command is passed to other peers in network. In this architecture each peer has the knowledge of neighbours, so command can easily receive and forwarded in the network. The figure shoes the architecture of the P2P Botnet.

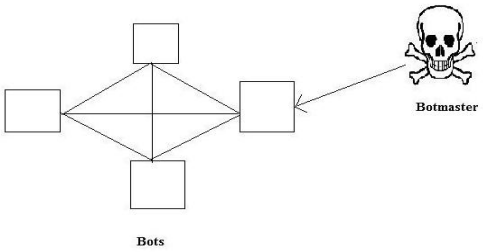

Fig. 2: Peer to Peer Architecture

In the figure the small rectangles shows the host in a peer to peer network. The botmaster gives command to one host and it will pass on to the other peers.

The types of attack is listed below which are done through the Botnet.

- Distributed Denial of Service (DDoS attack)
- Key logging
- Sniffing traffic
- Sniffing bandwidth
- Attacking IRC network
- Spamming
- Manipulating online Games
- Advertisement installation

III. TYPES OF BOTNET AND TOOLS

The table below shows the different types of Botnets and their characteristics [4].

Name	Originated	Characteristic
Nugache	Beginning of 2006	-One of the first to use strong cryptography to protect its communication. -used for DDoS attack.
Sality P2P	Early 2008	-Uses a pull-based unstructured p2p network to spread URLs where payloads are downloaded.
Kelihos	2010	-Used for spamming and ID Theft.
Zeus P2P		-Designed to steal the credential details from infected hosts.
Storm	January 2007	-structured P2P Botnet. -built upon an existing overnet network used for file sharing.
Miner	August 2011	-unstructured P2P Botnet. -included facility for generating digital currency "Bitcoin".

Table. 1: Types of Botnet

The above mentioned Botnets are the types of the P2P Botnets.

As per [2] there are three types of Botnet based DDoS attack, they are the agent-handler, IRC based, Web-based model.

In the agent-handler model the client communicate to the agent for performing the DDoS attack. Some other Botnet types are explained below.

Sdbot: It is discovered in April 2002. Sdbot is a Trojan horse that opens a back door and allows a remote attacker to control a computer by using Internet Relay Chat (IRC). It has affected Windows 95, 98, 2000, xp and Windows server 2003.

Agobot: Agobot is multithreaded and written in c++. Phatbot and Forbot are the family of the Agobot. It is used for targeting Microsoft Windows platforms. It has features like, remotely update and remove the installed bot, Execute programs and commands, Port scanner used to find and infect other hosts [10].

Phatbot: It is dynamically updated itself. Reboot, shutdown and logoff infected hosts. Download and Execute files using HTTP and FTP. Execute DDoS attack. It is derived from Agobot and uses client/server relationship.

The different tools of Botnet for creating attack are listed below.

These tools are mainly used for the DDoS attack. The tools are given the command for generating the traffic (Packet Flood) which crosses the limit of the server to handle the traffic and results denial of service.

There are no apparent characteristics of DDoS streams that could directly use for their detection [5]. The earlier DDoS attacks are used for fun but now it is used for intentionally for making money

Tool	Characteristic
TFN	UDP Flooding, TCP SYN Flooding, Smurf attack
Knight	IRC based tool for UDP Flood attacks & SYN attacks
BlackEnergy	Web based DDoS attack tool for deny service
TFN2K	Same characteristic as TFN and has an extra feature that it can add encrypted messages between attack components.
Trinity	TCP random flag packet floods, TCP RST packet floods.
Trinoo	Bandwidth depletion, UDP flood attacks.
kaiten	UDP-TCP flood attacks.
Mstream	point to point TCP ACK flooding
Low-Orbit Ion Cannon(LOIC)	Flooding in servers, generating HTTP traffic.

Table 2: Different Tools for Botnet creation.

IV. DETECTION OF BOTNET

It is very hard to detect the Botnet based attacks before they appear. Every time the attacker can generate the new code and techniques for performing the attack.

There are lots of researches going on for the detection of Botnet based attacks.

As per [6] the solutions for detection of the Botnet are Network based and Host based solution. In network based technique first step is to identify the C&C channel, after that finding out the infected host and the server. Once identified, actions are taken for stopping the malicious activity. In Host based solutions is to monitor the system and detect the malicious activity from inside.

There are active and passive methods for detecting active Botnets [7].

1). Active detection involves capturing live instances of running Botnets.

2). Passive detection involves capturing of live network malicious traffic.

The anti-Botnet Detection system includes four phases which are analysis, Detection, Mitigation, and Prevention [8]. The other methods for detecting Botnet is signature based and anomaly based technique.

A. Signature Based Detection:

In the signature based detection the research is conducted on the different Botnet for analysis and signature of the Bots. As the signatures are founded the AV companies include that signatures of Botnet in their software releases and make AV Users to update the software. So the normal users have to update the Anti-Virus (AV) software periodically. The limitation of the signature based method is that it cannot detect unknown attack. This technique can be included in Host Based Detection.

B. Anomaly Based Detection:

Anomaly detection simply aims to detect significant variation from normal behaviour. This technique includes changes into the file system, system behaviour, and unknown processes. It overcomes some drawbacks of Signature based detection. The advantage of anomaly based detection is that it is good at discovering new system infection [9].

C. Botnet Fast Flux Detection Technique:

Holz et al. have develop a metric to detect fast-flux service network which identifies the number of IP domain filters,

number of name server records, and number of autonomous systems in all IP-domain pairs[15].

V. BOTNET DEFENCES

For defence against the Botnet first step is to cut the communication channel of the machine. Then remove the malware and update the system. Defender has to develop an automated notification system to detect and remove the Botnet [11].

A. Honeypot- Based Monitoring: One of the best techniques for detecting the Botnet is to create a honeypot for the attacker. The honeypot is simply a virtual environment which attracts the attacker for attack. Using Honeypot we can trap the attacker and can save the system from attack. It is widely used for monitoring the Botnet activity. The honeypot based monitoring is done globally; so many researchers are joined together from different countries and contribute against the Botnet [12].

B. SHIVA (Spam Honeypot with Intelligent Virtual Analyzer): SHIVA is an open-source and developed in Python2.7. Analysis of data captured can be used to get information on phishing attacks, scamming campaigns, malware campaigns, spam botnets, spammer's identity [13]. SHIVA source code is available at https://github.com/shiva-spampot/shiva.

VI. CONCLUSION

Botnets are the new weapon for the hacker community for making money and stealing information. The different types of botnets have different characteristics and when new Botnet arrive it has some new signatures. So AV companies have to update everyday against these activities and have to develop new techniques for detecting them.

In this paper we have discussed some types of botnets and their characteristics, some tools for generating bots and detection techniques. Botnet field needs more research for stopping the attacks and needs more research on anomaly based detection.

REFERENCES

[1] Sanket N Patel, Tarulata Chauhan "Glimpse of Bonet: Analysis, Detection and Defense"
[2] Esraa Alomari, Selvakumar Manickam, B.B.Gupta, Shankar Karuppayah, Rafeef Alfaris "Botnet-based Distributed Denial of Service(DDoS) Attacks on Web Servers: Classification and Art"
[3] Gunter Ollmann "Botnet Communication Topologies"
[4] Christian Rossow, Dennis Andriesse, Tillmann Werner, Brett Stone-Gross, Daniel Plohmann, Christian J. Dietrich, Herbert Bos "SoK: P2PWNED— Modeling and Evaluating the Resilience of Peer-to-Peer Botnets"
[5] Christos Douligeris, Aikaterini Mitrokotsa "DDoS attacks and defense mechanisms:classification and state-of-the-art"
[6] Areej Al-Bataineh, Gregory White "Detection and Prevention Methods of Botnet-generated Spam"
[7] Jivesh Govil, Jivika Govil "Criminology of BotNets and their Detection and Defense Methods" IEEE EIT 2007 Proceedings
[8] Jan Kok, Bernhard Kurz "Analysis of the BotNet Ecosystem" CTTE 2011 · 16-18 May, 2011, Berlin, Germany
[9] Gregory Fedynyshyn, Mooi Choo Chuah, Gang Tan "Detection and Classification of Different Botnet C&C Channels"
[10] "Agobot-Wikipedia, the free encyclopedia"
[11] Chao Li, Wei Jiang, Xin Zou "Botnet: Survey and Case Study" 2009 Fourth International Conference on Innovative Computing, Information and Control
[12] http://www.honeypot.org
[13] https://github.com/shiva-spambot/shiva
[14] Lei Zhang, Shui Yu, Di Wu, Paul Watters "A Survey on Latest Botnet Attack and Defense" 2011 International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11

.

