ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 3, March 2015**

# Review of Botnet Attacks and its Detection Mechanism

D.Kavitha[1], Rani S.K[2]

Assistant Professor, Dept. of CSE, Valliammai Engineering College, Chennai, India

PG Scholar, Dept. of CSE, Valliammai Engineering College, Chennai India

**ABSTRACT:** Criminal communities share strategies and tools and can combine forces to launch coordinated attacks. They even have an underground marketplace where cyber criminals can buy and sell stolen information and identities. It's very difficult to crack down on cyber criminals because the Internet makes it easier for people to do things anonymously and from any location on the globe. Botnet is one of the significant types of attack technique used by hackers. It is a network of hijacked computers that a hacker controls remotely to send spam or launch cyber-attacks. It spreads quickly and becoming more resilient, so it's critical to identify and respond to them promptly. This paper focuses on Botnet attacks and its detection strategies.

**KEYWORDS**: Botnets; Botnet Detection; Cyber Security; Centralized Bots; P2P Bots;

## I. INTRODUCTION

Hackers constantly researched about weakness in computer networks more effectively. Through the creation of networks of controlled computers, hackers launch attacks on the internet. "Bot" is actually short for robot, not the kind found in science fiction movies or on the production line in a manufacturing business. Bots are one of the most sophisticated types of crime-ware facing the Internet today. Bots [1] are similar to worms and Trojans, but earn their unique name by performing a wide variety of automated tasks on behalf of their master (the cybercriminals) who are often safely located somewhere far across the Internet. Botnet operators have consequently developed a range of technologies and tactics to protect their C&C investment. Botnet Trojan Horses can be considered as one of the newest threats to the Internet. This type of Trojan was first introduced across the internet in the late 90's [2]

The Trojan architecture is highly similar to that of initial Trojans, but their purpose and the way they operate in the network is significantly different from those initial types of attacks, both in intent and in procedure. Botnets can infect a few systems and up to several million computers in a network in order to obtain valuable data regarding individuals and organizations. One of most recent research works performed by the Kaspersky lab team it has become clear that targets are normally chosen from businesses and not personal users; though personal computer users can also be affected by Trojans.

## II. TYPES OF BOTNET

Bots can be classified into many types depending upon the communication protocol used or its hierarchy. The two typical types of botnet based upon hierarchy are

1. Centralized C&C
2. Peer to Peer (P2P) bots.

The above life cycle is an example of a bot with centralized server. Bots with centralized C&C are easy to deploy and administer for the bot master. It suffers from a single point of failure i.e. if the C&C is brought down by the network administrators; the bots are isolated from the bot masters. The bots no longer can communicate with the master and become group of infected machines. Recently, the bot masters have come up with a technique called fast flux to overcome this issue. Fast flux is a DNS technique which hides the address of C&C behind a network of compromised machines which act as proxy servers.

In P2P bots [3] commands are communicated through push/pull mechanism. Bot master publishes a command file over the P2P network. The bots then use the pull mechanism to obtain the command file. P2P bots have constantly

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

communicates with its neighbors for commands and has to send KEEP ALIVE messages to other bots in the network. P2P botnets do not suffer from single point of failure but coordination of bots is difficult compared to the centralized architecture.

## III. LIFE CYCLE OF BOTNETS

The life cycle of an IRC based bot is explained as follows

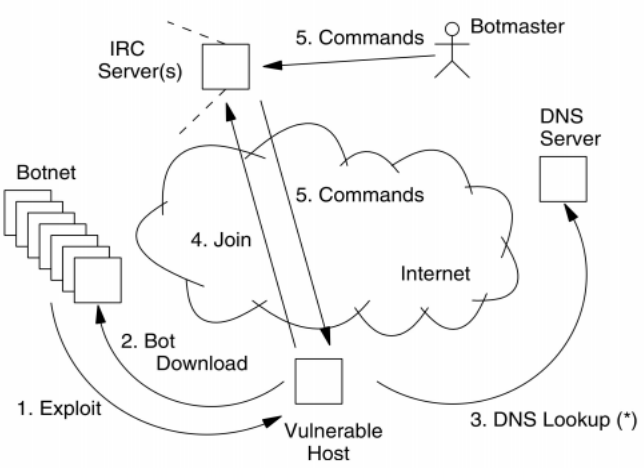


**Fig.1 Botnet Life Cycle**

It begins with the infection stage. The exploitation of victim computer can be due to any one of the following reasons.

1. Unpatched vulnerabilities.
2. Backdoors left by trojans
3. Password guessing and brute force attacks.

The infected machine is called a zombie or a drone. Once a host is infected, it downloads the bot binary source from a remote server and installs automatically. The bot then looks up for the address of IRC servers by DNS Lookups. These IRC servers are called Command and Control (C&C) servers.

On obtaining the C&C server's address, the bot then logs into it and authenticates itself as a part of the particular botnet. The bots can then update their bot software this is usually functionalities added to the bot software, if an update were available and add more C&C servers. IRC servers are used for C&C by bot masters is due to the following reasons.

- Easy to install i.e. private network can be installed easily.
- Easy to control i.e. using features like username, passwords.
- Interactive i.e. two way communication between bot master and zombie machine is possible.

These zombie machines, when it is up and connected to the Internet, will log into the C&C server and wait for bot master's commands. Bot master logs into the C&C and can now issue commands for the bots to perform.

## IV. BOTNET TOPOLOGY

Botnet Topology can be Classified into, 1) Star, 2) Multi Server, 3) Hierarchical, 4) Random.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

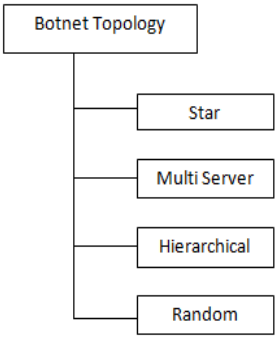


**Fig.2 Botnet Topology**

### 1. Star

The Star topology relies upon a single centralized C&C resource to communicate with all bot agents. Each bot agent is issued new instructions directly from the central C&C point. When a bot agent successfully breaches a victim computer, it is normally preconfigured to "phone home" to this central C&C, whereupon it registers itself as a botnet member and awaits new instructions.

### 2. Multi Server

Multi-Server C&C topology is a logical extension of the Star topology, in which multiple servers are used to provide C&C instructions to bot agents. These multiple command systems communicate amongst each other as they manage the botnet. Should an individual sever fail or be permanently removed, commands from the remaining servers maintain control of the botnet. It takes more planning and effort on the part of the botnet's operator to construct a Multi-Server C&C. However the same bot agents can be used for both Star and Multi-Server topologies. Intelligent distribution of the multiple C&C severs amongst different geographical locations can speed up communications with similarly located bot agents. Likewise, C&C servers simultaneously hosted in multiple countries can make the botnet more resistant to legal shutdown requests.

### 3. Hierarchical

A Hierarchical topology reflects the dynamics of the methods used in the compromise and subsequent propagation of the bot agents themselves. Bot agents have the ability to proxy new C&C instructions to previously propagated progeny agents. However, updated command instructions typically suffer latency issues making it difficult for a botnet operator to use the botnet for real-time activities. A Hierarchical botnet means that no single bot agent is aware of the location of the entire botnet. This configuration makes it difficult for security researchers to estimate the overall size of the botnet. The Hierarchical structure also facilitates carving up larger botnets in to sub-botnets for sale or lease to other botnet operators. Hierarchical topologies can facilitate a mix of propagation tactics – e.g. an initial drive-by download infection that then initiates worm capabilities once established inside an enterprise network.

### 4. Random

Botnets with a Random topology (i.e., a dynamic master-slave or peer-to-peer relationship) have no centralized C&C infrastructure. Instead, commands are injected in to the botnet via any bot agent. These commands are often "signed" as authoritative, which tells the agent to automatically propagate the commands to all other agents. Random botnets are highly resilient to shut down and hijacking because they lack centralized C&C and employ multiple communication paths between bot agents. However, it is often easy to identify members of the botnet by monitoring a single infected host and observing the external hosts it communicates with. Command latency is a problem for Random topology botnets. However, the multiple communication links between bots agents make latency less of a problem than with Hierarchical topologies.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

## V. BOTNET DETECTION TECHNIQUES

### 1. Botminer

Botminer proposed in [4], is an improvement of Botsniffer applying data mining techniques for Botnet C&C traffic detection. Firstly, similar communication traffic and similar malicious traffic are clustered. Then, cross cluster correlation are performed to identify the hosts that share both similar communication patterns and similar malicious activity patterns. Botminer is an advanced Botnet detection tool which is independent of botnet C&C protocol and structure, and requires no a priori knowledge (e.g C&C addresses/signatures) of specific botnets. It can detect both centralized (e.g., IRC, HTTP) and current (and possibly future) P2P based botnets. Although Botminer are not dependent on a specific protocol and botnets network topology, a lot of calculation of cluster analysis are needed and it is difficult to ensure the accuracy and real-time.

### 2. Signature-based Detection

Knowledge of useful signatures and behavior of existing botnets is useful for botnet detection. For example, Snort [5] is an open source intrusion detection system (IDS) that monitors network traffic to find signs of intrusion. Like most IDS systems, Snort is configured with a set of rules or signatures to log traffic which is deemed suspicious [5]. However, signature-based detection techniques can be used for detection of known botnets. Thus, this solution is not useful for unknown bots.

### 3. Active monitoring:

Active monitoring strategy detects botnets through actively injecting packets into the network or using network crawlers. For instance, an active crawler proposed in [6] can collect the location information from all participants and actively identify the bots of all the Storm Worm botnets. Compared with another active method for identifying Storm bots [7], the crawler in [6] is more efficient because it introduces more protocol-based messages to collect information about peers.

### 4. C&C Server Hijack:

Bots can be actively detected by C&C server hijack. Bots report to and receive commands from C&C server. Taking control of the C&C server will reveal all the bots that contact it. This can be achieved by exploiting botnet rallying mechanism. A defender can use this information to his/her advantage to hijack the server. This approach also leverages knowledge of botnet topology. Centralized botnet structures are more amenable to C&C server hijack. In decentralized botnets, the C&C server can be any peer and will, at most, reveal information about bots in its peer list. To gain further information, some other techniques need to be employed, such as active crawling of the p2p botnet. The seizure of C&C servers can be Physical or Virtual.

#### 4.1 Physical Hijack

In a Physical hijack, law enforcement agencies physically seize the C&C servers. However, it is possible to take over the C&C servers without involving legal authorities by mutual cooperation. This is possible if the C&C servers in question are not in geographically diverse locations. With the help of service providers, researchers gained access to several C&C servers used by Push do/ Cutwail botnet [8]. In addition to other interesting information, 24 databases containing details about the bots and spam operations were disclosed.

#### 4.2 Virtual Hijack

In a *Virtual* take over, defenders hijack the C&C servers by redirecting C&C communication to a machine under their control. This technique has been used by researchers to hijack botnets that use domain names for rallying. By virtue of DNS sink holing, traffic sent by bots to known botnet domains can be forwarded to defender-controlled machine. The domain names of C&C servers can be learnt by analyzing the botnet

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

behavior on infected machines. Researchers [9], [10] have recovered future rendezvous points by reverse engineering the domain generation algorithm used by botnets utilizing domain flux.

**5. Botsniffer**

Botsniffer [11] that uses network-based anomaly detection to identify botnet C&C channels in a local area network. Botsniffer is based on observation that bots within the same botnet will likely demonstrate very strong synchronization in their responses and activities. Hence, it employs several correlation analysis algorithms to detect spatial-temporal correlation in network traffic with a very low false positive rate [11].

**6. Operational Behavior Analysis:**

Unlike the method mentioned above, operational behavior analysis focuses on bots' characteristics, C&C servers and communication methods, botmaster behavior and intentions. Therefore, a number of studies on botnet detection have adopted behavioral analysis by collecting the network traffic for a specific period (i.e. passive approach) and analyze them in order to identify any evidence of bot and botnet activities [12].

**7. BotHunter**

In BotHunter [13], bot infection pattern are modeled to use for recognizing the whole process of infection of Botnet in the network. All behavior that occur the bot infection such as target scanning, C&C establishment, binary downloading and outbound propagation have to model by this method. This method gathers an evidence-trail of connected infection process for each internal machine and then tries to look for a threshold combination of sequences that will convince the condition for bot infection. The BotHunter uses snort with adding two anomaly-detection components to it that are SLADE (Statistical pay Load Anomaly Detection Engine) and SCADE (Statistical scan Anomaly Detection Engine).

**8. Detection via cooperative behaviors**

(i) Karasaridis et al. designed a detection scheme to calculate the distances between monitored flow data and a pre-defined IRC traffic flow model [14].

(ii) Ramachandram et al. discovered identities of bots based on the insight that botmasters themselves must perform ”reconnaissance” lookups to determine their bots' blacklist status [15].

(iii) Strayer et al. proposed a temporal correlation algorithm in a five-dimensional space about packet inter-arrival time and packet size [16].

**9. Mining Based Detection**

Masud *et al.* [17] proposed robust and effective flow-based botnet traffic detection by mining multiple log files. They introduce multiple log correlation for C&C traffic detection. They classify an entire flow to identify botnet C&C traffic. This method does not impose any restriction on the botnet communication protocol and is therefore applicable to non-IRC botnets. Furthermore, this method does not require access to payload content. Hence, it is effective even if the C&C payload is encrypted or is not available [17].

**10. Network Based Detection:**

In 2007, Choi et al. [18] suggested anomaly mechanism by monitoring group activities in DNS traffics. They defined some special features of DNS traffics to differentiate valid DNS queries from Botnet DNS queries. This method is more efficient than the prior approaches and can detect Botnet despite the type of bot by looking at their group activities in DNS traffic [18].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 3, March 2015**

### 11. Honeypot and Honeynet

Honeypots are tools that are used as traps to collect the bots' information and activities and analyses them in order to detect botnets. The information can be used to understand more about bots' behavior or the intentions of the botmaster [19]. There are two types of Honeypots: low-interaction honeypots and high-interaction honeypots [20]. The main difference between them is the level of access rights to system resources, services, and functions [21]. Low-interaction honeypots are deployed with a limited interaction between computers and botmaster. Therefore they may not be completely compromised and the collected information may not be sufficient for analysis to detect botnets. In order to provide more information, the high-interaction honeypots emulate the real system and services which allow botmaster to have more control. Although this approach is able to provide useful information for botnet detection, the botmaster can gain full control of the computers in which the high interaction honeypot is installed. Moreover recently botmasters use many techniques to detect and avoid the honeypots [22].

## VI. CONCLUSION AND FUTURE WORK

Some hackers targets organizations that store people's personal information, like credit card companies. But most cyber criminals will target home computers rather than trying to break into a big institution's network because it's much easier. Many computers used in cyber-attacks have actually been hacked and are being controlled by someone far away. By taking measures to protect your personal information, you are not only preventing cyber criminals from stealing your identity, but also protecting others by preventing your computer from becoming part of a botnet. Botnet change their communication architecture consequently. This dynamic nature of botnet makes their detection a challenging task. This survey provides entire detection techniques of Botnets and it is very helpful for all kinds of environment. It also creates user awareness.

## REFERENCES

1. http://searchsecurity.techtarget.com/definition/botnet.
   Botnet: 10 Years of Security Threats. Retrieved September 06, 2009, from MalwareCity: MalwareCity.com.
2. https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/grizzard/grizzard_html/index.html
3. G. Gu, R. Perdisci, J. Zhang, and W. Lee, "Bot miner: Clustering analysis of network traffic for protocol and structure independent Botnet detection," in Proc. 17th USENIX Security Symposium, 2008.
4. Snort IDS web page. http://www.snort.org, March 2006.
5. BinbinWang, Zhitang Li "Actively Measuring Bots in Peer-to-Peer Networks," in Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC '09.
6. T. Holz, M. Steiner, F. Dahl, E. W. Biersack, and F. Freiling, "Measurements and mitigation of peer-to-peer-based botnets: A case study on storm worm", in Proc. of the 1st Usenix Workshop on Largescale Exploits and Emergent Threats (LEET '08) , 2008.
7. B. Stone-Gross, G. S. T. Holz, and G. Vigna., "The underground economy of spam: A botmasters perspective of coordinating largescale spam campaigns," in USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2011
8. S. Shin and G. Gu, "Conficker and beyond: A large-scale empirical study," in Proc. Annual Computer Security Applications Conference (ACSAC), 2010
9. B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szyd-lowski, R. Kemmerer, C. Kruegel, and G. Vigna, "Your botnet is my botnet: Analysis of a botnet takeover," in Proc. 16th ACM conference on Computer and Communications Security *(CCS)*, Nov 2009
10. G. Gu, J. Zhang, and W. Lee, "Botsniffer: Detecting botnet command and control channels in network traffic," in Proc. 15th Annual Network and distributed System Security Symposium (NDSS'08), 2008.
11. M. Bailey, E. Cooke, F. Jahanian, X. Yunjing, and M. Karir, "A Survey of Botnet Technology and Defenses," in Proceedings of the Cybersecurity Applications & Technology Conference for Homeland Security (CATCH), 2009, pp. 299-304.
12. G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee. BotHunter: Detecting malware infection through ids-driven dialog correlation. In Proceedings of the 16th USENIX Security Symposium (Security'07),2007.
13. A. Karasaridis, B. Rexroad, and D. Hoeflin. Wide-scale botnet detection and characterization. In First Workshop on Hot Topics in Understanding Botnets (HotBots'07), Cambridge, MA, April 2007
14. A. Ramachandran, N. Feamster, and D. Dagon. Revealing botnet membership using dnsbl counter-intelligence. In Proceedings of the 2nd conference on Steps to Reducing Unwanted Traffic on the Internet (SRUTI'06), San Jose, CA, July 2006.
15. W. T. Strayey, R.Walsh, C. Livadas, and D. Lapsley. Detecting botnets with tight command and control. In 31st IEEE Conference on Local Computer Networks (LCN06), Tampa, Florida, November 2006
16. M. M. Masud, T. Al-khateeb, L. Khan, B. Thuraisingham, K. W. Hamlen, " Flow-based identification of botnet traffic by mining multiple log file," in Proc. International Conference on Distributed Frameworks & Applications (DFMA), Penang, Malaysia, 2008.
17. H. Choi, H. Lee, H. Lee, and H. Kim, "Botnet Detection by Monitoring Group Activities in DNS Traffic," in Proc. 7th IEEE International Conference on Computer and Information Technology (CIT 2007), 2007,pp.715-720.
18. P. Wang, L. Wu, R. Cunningham, and C. Zou, "Honeypot Detection in Advanced Botnet Attacks," International Journal of Information and Computer Security, vol. 4, pp. 30-51, 2010.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 3, March 2015**

19. W. Zanoramy, A. Zakaria, and M. L. M. Kiah, "A Review on Artificial Intelligence Techniques for Developing Intelligent Honeypot," in Proceedings of the 3rd International Conference on Next Generation Information Technology (ICNIT), Seoul: Korea, 2012, pp. 696-701.
20. N. Provos and T. Holz, "Virtual Honeypots: From Botnet Tracking to Intrusion Detection, 1st ed. Addison Wesley Professional, 2007
21. A. K. Seewald and W. N. Gansterer, "On the Detection and Identification of Botnets," Computers & Security, vol. 29, pp. 45-58, 2010.