*International Journal of Computer Applications (0975 – 8887)*
*Volume 75– No.7, August 2013*

# Survey and Research Challenges of Botnet Forensics

Anchit Bijalwan*, Meenakshi Thapaliyal, Emmanuel S Pilli, R.C.Joshi
Department of Computer Science & Engineering
Uttarakhand Technical University*, Graphic Era University, Dehradun, India

## ABSTRACT

Botnet has recently been recognized as one of the most significant security threats/worms of the Internet. Latest attacks are increasingly complex, and utilize many strategies in order to perform their intended malicious/hazardous task. Attackers have developed the ability of controlling vast area of infected hosts, characterized by complex executable command set, each involved part in cooperative and coordinated attacks. These papers propose the advanced approach related botnet detection and analysis in the near future. It demonstrates a novel approach of botnet investigations and defense mechanisms.

## Keywords

Bots, Botnet, C&C, Analysis

## 1. INTRODUCTION

Currently, Computer networks and hosts have always been under attack by computer-generated problems. Bot, malicious software have been global crisis. A network of bots constitutes a botnet which is a potent general purpose distributed supercomputer. Botnet represent a very serious threat to the Internet security because they can be used to initiate massive attacks against which there are no effective mitigation strategies. The Botnet is a network of large number of the infected end host called Bots which is controlled by a remote human operator called "Botmaster". A bot is installed in a compromised machine and botmaster operates the bots via command and control(C&C). The term 'bot' is used to denote a computer that is infected by malicious code which often exploits software vulnerabilities on the computer to allow a malicious get-together commonly denoted as 'botherder' to control the computer from a remote location without the user's knowledge and consent [1].

Once infected with a bot, the victim host will join a botnet, which is a network of compromised machines that are under the control of a malicious entity, typically referred to as the botmaster. Botnets are the primary means for cyber-criminals to carry out their nefarious tasks, such as sending spam mails, launching denial-of-service attacks, or stealing personal data such as mail accounts or bank credentials. This reflects the shift from an environment in which malware was developed for fun, to the current situation, where malware is spread for financial profit. Denial-of-service (DoS) attacks, phishing, spamming, key logging, click fraud, identity theft and information exhilaration is main hazardous behavior which associated with the botnet. Botnets apply a self-propagating function to infected hosts. Given the importance of the problem, significant research effort has been invested to gain a better understanding of the botnet phenomenon.

Botnet detection: It is the technique of detecting a bots from the network. Botnet detection is strategies broadly divided into two types[2]:

Host based approach: Detecting bots activities on a single machine.
Network based approach: Detecting bots activities on a network.

One approach to study botnets is to perform passive analysis of secondary effects that are caused by the activity of compromised machines [3]. For example, researchers have collected spam mails that were likely sent by bots. It is collecting the data through monitoring activities can be tracked without interfering with the environment or tampering with the evidence. Other researchers analyzed IRC traffic, capable of identifying botnet related activities. A more active approach to study botnets is via infiltration. It contains approaches that involve interaction with the information sources being monitored Infiltration of botnets can be divided into: software and hardware based techniques. The first covers research on the bot executable and monitored traffic to achieve control and conduct measurements. The latter can be applied if access to the command-and-control server is possible and may be used to wiretap the communication. According to the command and control (C&C) models, botnets are separated into two groups of centralized (e.g., IRC and HTTP) and distributed (e.g., P2P). Centralized botnet utilize two mechanisms to get the command from the server, which is push and pull. In the push system, bots are associated to the C&C server (e.g., IRC server) and wait for the commands from the botmaster. In contrast, in the pull mechanism, the botmaster sets the commands in a file at C&C server (e.g., HTTP server), and the bot often connect to the server to read the most recent commands. While in centralized structure all bots receive the commands from a definite server, in distributed structure the command files will be mutual over P2P networks by botmaster, and bots can use explicit search keys to find the available command files [4].

Botnet Analysis is to determine the path from a victim network or system through any intermediate systems and communication pathways, back to the point of attack origination

Static Analysis: Static analysis /White box testing is the process of understanding the behaviour of a program without executing it. The analysis checks the presence of viruses in file system such as firewall logs.

Dynamic Analysis: Dynamic Analysis / Black box testing differs from static analysis. Analyzing the actions performed by a program while it is being executed is called dynamic analysis[5]. How, what and where is done by bots, that is botnet forensics Analysis. Forensic is a discipline based on science & technology to investigate and establish facts in criminal & civil courts. It deals with collecting, analyzing and helps in presenting evidences in a court of law. Network forensics is the science that deals with capture, recording, and analysis of network traffic for detecting intrusions and investigating them [6].

The rest of paper is organized as following. Section 2 introduces the botnet life cycle and structure, Section 3 research related studies, section 4 defines model of botnet forensics, botnet defense technique which is required by mitigation of botnet is detail in Section 5, and some researchers' challenges in Section 6, and at last, we discuss conclusion and future directions in Section 7.

## 2. BACKGROUND AND MOTIVATION

Bot, botmaster and C&C are the basic elements of the botnet. These elements play a significant role in survive of botnet. There are five phases in involve a botnet life cycle [7] .

Primary infection is the first phase of botnet life cycle, where in a host is infected and becomes a possible bot. This phase is characterized by a expected computer infection procedure, which may be passed away in different behavior as a typical virus infection would be, for instance, through unwanted downloads of malware from websites, infected removable disks, infected files attached to email messages, etc.

Second phase is defined the secondary injection, Firstly, the first phase be successfully finished. In this phase, the infected host runs a program that searches for malware binaries in a given network database. When downloaded and executed, these binaries make the host behave as a zombie). Downloading bot binaries is usually performed by FTP, HTTP or P2P protocols.

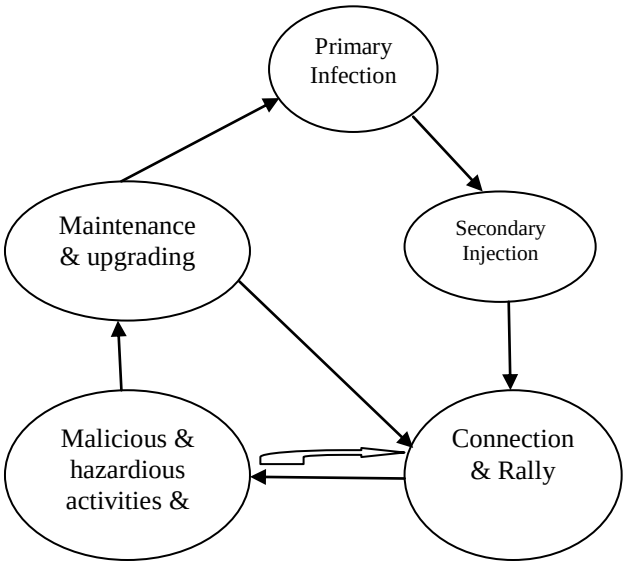


**Fig. 1 Botnet Life Cycle**

Third phase is scheduled every time the host is restarted to ensure the botmaster that the bot is taking element in the botnet and is capable to receive commands to perform malicious activities. After establishing the command and control channel the bot waits for commands to perform malicious activities.

Phase 4 is ready to perform an attack. Malicious /Hazardous activities may be as broad ranging as information theft, performing DDoS attacks, extortion, monitoring network traffic, spreading malware, stealing computer resources, and unprotected computers, identity theft, phishing, spamming, manipulating games and surveys, etc. Phase 5 Maintenance and up gradating is the most important phase of botnet life cycle. Maintenance is necessary if the botmaster wants to keep his army of zombies. It may be necessary to update codes for many reasons, including evading detection techniques, adding new features or migrating to another C&C. This phase is also usually measured a susceptible step. As the botmaster intends to broadcast updates as soon as possible, some behavioral patterns of the stations belonging to the network may emerge and make the botnet detectable. Changes in behavior are typically observed, for instance, in DNS queries and file sharing, among other areas. After bots are updated, they must establish new connections with the C&C infrastructure.

Botnets, networks of malware infected machines controlled by an adversary, are the root cause of a large number of Internet security problems.

## 2.1 Proliferation and Motivation

Botnet infected system can infect other machines connected to it. System used to conduct packet floods, attackers surreptitiously install their malicious software which getting malicious software on victim's hosts has evolved significantly over time [8]. Modification that happened a once is the move from a single propagation vector, that might have required a manual installation process by the attacker, to multiple automated propagation vectors. For example, The Slammer worm used a single vulnerability to infect hosts while more modern bots have many distinct, completely automated propagation vectors / SDBot ( rBot) propagates using a number of different mechanisms including open files shares, P2P networks, backdoors left by previous worms, and using exploits of numerous common Windows vulnerabilities.

## 2.2 C& C (Command And Control)

Communication is the next major problem of the botnet attacker. Most attackers would communicate to bots but do not interact to the exposed bots. Botnet has three potential topologies to explore of various bot communication methods:

Centralized:

A centralized topology is characterized by a central point that communicates among clients. Malicious IRC botnet /HTTP botnet is typical Centralized botnet [9]. They can be easily detected since many Clients connect the same point, and it can be stopped activity of botnet with blocking C&C. Usually consisting of a central node distributing messages between network clients. They are characterized by:

- Low latency due to the small number of hops required to transmit the orders from the botmaster.
- Direct connection to order distribution nodes, which would compromise the security of the network in case of accidental detection of a node.
- Implemented using different communication protocols, but most typically the IRC and HTPP.

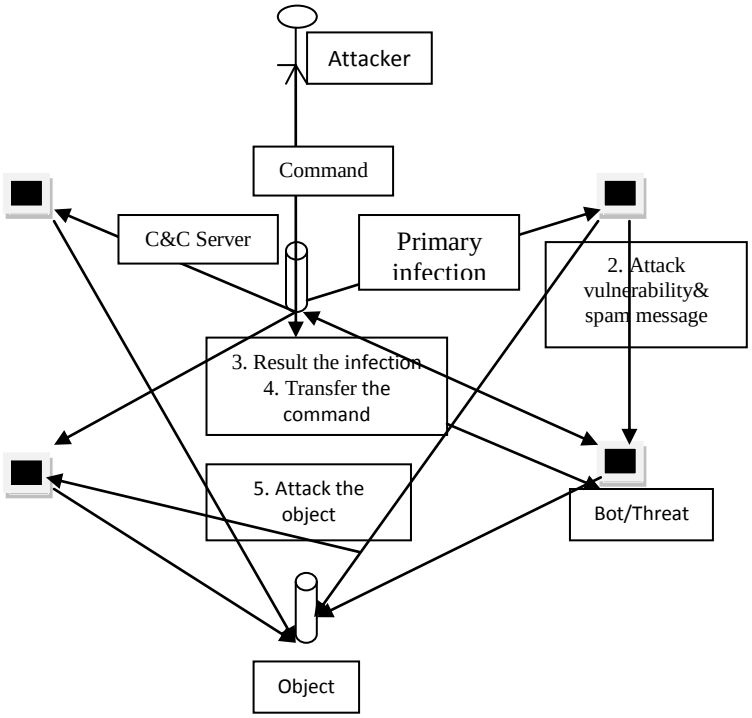


**Fig. 2 Centralized botnet structure**

## Peer to Peer:

P2P topology has not Command &C control server. In a peer to peer architecture a node can act as both client and server and there is lack of centralized point for command and control. Peer to Peer is a P2P communication system is much strong, complex and typically no guarantees on message delivery or latency. Transferring command of P2P botnet is a slow to compare with centralized botnet. This means that the compromise of a single bot does not necessarily mean the loss of the entire botnet. e.g., Peacomm, Mega-D, Waledac etc.

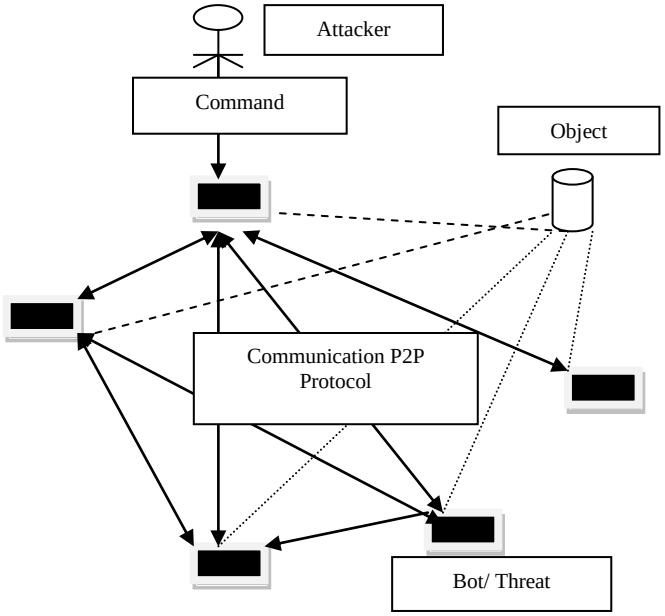


**Fig. 3 Peer to Peer botnet structure**

A P2P botnet do not requires formal coordination and even if a node is taken offline by the defender, the network still remains under the control of the attacker. A botmaster transfer command to a bot peer, a command spreads all zombie peers by communication between each other. They have the advantage of being more difficult to destabilize as they do not have a unique core from which issuing orders and/or sharing resources and information, making use of the facilities of traditional P2P networks which allow a high connection and disconnection ratios [10]. Each node has greater structural complexity because all of them can act as both, client and server, being more difficult to intercept and study.

## Hybrid:

A hybrid peer-to-peer botnet based on the unstructured P2P protocols[11]. A hybrid botnet will be divided into servent and client bot. The servent bot receives the commands from the bot master, and it forward to the client. Example is the Nugache botnet (2006). The hybrid P2P botnet is equivalent to a C&C botnet where servent bots take the role of C&C servers: the number of C&C servers (servent bots) is greatly enlarged, and they interconnect with each other. In hybrid P2P botnet in comparision in current botnet is harder to shut down monitored and hijacked[12].

## 2.3 Attacks and Theft

The next core problem for botnet attackers is how to extract value from a bot infected node. Botnets used to initiate simple DoS (denial of service) attacks quickly evolved into multi-host distributed DDoS attacks involving large numbers of computers. SDBot and Agobot both have remotely accessible commands for

network in which any node in a network can act as both a client and a server.P2P botnets aim at removing the failure point which is the main limitation and vulnerability of centralized networks [8,9]

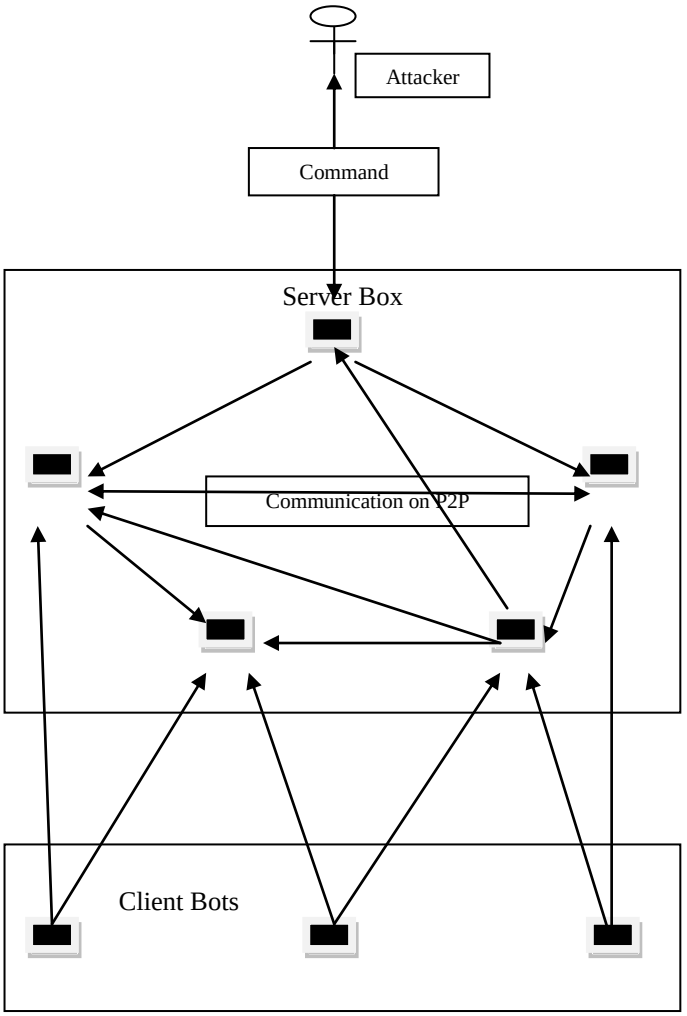


**Fig.4 : Hybrid botnet structure Through P2P and Client Bots**

card/social security numbers, and other personal information for identity theft and to commit industrial intelligence. Example like advanced key logging techniques to collect private information is SDBot.

initiating DDoS attacks. Botmaster find out the information stored on infected computers/the networks. Attackers can use stolen credit

## 3. STATE – OF – ART

Botnets have recently gained high interest by the scientific area, media and industry. In recent year there have been many approaches to analyze botnet behaviors.

Mused *et al.* [14] proposed a multiple log-file based temporal correlation technique for detecting C&C traffic. Main assumption is that bots respond much faster than humans. They applied log files technique produced by tcpdump and exedump, which recall all incoming and outgoing network packets and the start times of application execution at the host machine. The naval idea of correlating multiple log files and applying data mining for detecting botnet C&C traffic. They implement a prototype system and evaluate its performance through different classifiers as Support Vector machine, decision tree, ByesNets, Boosted decision tree and Naivy.

Botmaster command categories can be used to detect control and command traffic and show the C&C payloads are not directly available.

Kalakota *et al*. [15] proposed Dynamic Early Filtering of Internet Traffic (DEFT), a novel approach which encodes unwanted traffic filtering rules. They implemented Quagga routing software which consists four major components, namely rule generation component, rule dissemination component, rule management component, and rule security component. The experimental results show that DEFT can effectively mitigate the impacts of malicious unwanted traffic to ensure efficient network utilization by the legitimate traffic.

DEFT is designed to be a comprehensive and sustainable framework that coordinates the routers in the Internet to achieve early filtering of malicious unwanted packets in Internet traffic. It is expected that the DEFT framework can have the offending unwanted traffic filtered early and so can bring about the benefits of reduced latency and increased throughput for legitimate traffic. However, the benefits are not always guaranteed along with the deployment of DEFT. If the DEFT is not appropriately configured, the benefits may be relatively small. This is mainly due to the cost of filtering: a router's action of filtering packets against a rule will incur extra packet processing overhead, and all the packets, no matter unwanted packets or good packets, need to be matched against the installed rules.

Wei *et al*. [4] proposed BotCop, advanced generic online botnet traffic classification system. Setting up and installing honeypots on the Internet is very helpful to capture malware and understand the basic behavior of botnets, and, as a result, makes it possible to create bot binaries or botnet signatures. BotCop into different application communities by using payload signatures /a novel decision tree model, and then on each obtained application community, the temporal-frequent characteristic of flows is studied and analyzed to differentiate the malicious communication traffic created by bots from normal traffic generated by human beings. The major contributions of this paper include:

(1) Propose a novel application discovery approach for automatically classifying network applications on a large scale WiFi ISP network;

(2) Develop a generic algorithm to discriminate general botnet behavior from the normal network traffic on a specific application community, which is based on *n*-gram (frequent Characteristics) of flow payload over a time period (temporal characteristics).

Li *et al*. [16] focused on all phases of botnets as Spreading, Forming, Waiting for Commands. Network traffic and honeypots is novel approach to monitor and analysis of P2P lifetime. The network traffic monitoring and analysis approach is useful to identify the existence of botnet in the networks. Kademlia, a new botnet protocol is designed a realistic method to deal with index poisoning in this protocol. The new botnet over this protocol is called Overbot. Simulation tests were operated to evaluate the performance of index poisoning attack**.** To simulate a P2P botnet with 4000 nodes, time in the simulated network is moving 60 times is faster than normal, By using index poisoning technique. It is at least more effectively to mitigate P2P botnets than before.

Dae-il *et al*. [9] studied the malicious HTTP2P botnet. Malicious botnet is evolving very quickly and using the many ways to evade detection system. The change of protocol is the most important part of the malicious botnet's evolution and evasion techniques. The initial malicious botnet was using the IRC protocol for communication between the command and control server and the zombie system. After that they use the HTTP protocol on the firewall-friendly and the P2P protocol to escape Client/Server architecture. During investigation of waledac was to find out more about the actual size of botnet.

Igor Kotenko *et al*. [17] proposed an approach of botnet simulation and defence in the Internet. It is examined by interaction of different agents teams. Environment for the agent-oriented simulation was developed on the basis of OMNeT++ INET Framework. Botnet defence can be considered in two main categories botnet detection/response techniques and measurement.Agent-based simulation of cyber attacks and cyber–defence mechanisms which combines discrete-event simulation, multi-agent approach and packet-level simulation of network protocols. The investigation of attack and defence scenarios has been finished on the basis of analysis of two main classes of parameter: the amount of incoming attack traffic before and after the filter team which network is the attack victim, false positive and false negative rates of attack detection. This paper shows the best result on blocking the attack traffic. This software simulation environment has been used to investigate various cooperative distributed defence mechanisms.

Borgaonkar *et al* .[1] studied the design and structure of the Asprox botnet. They investigated the C & C structure used by Asprox botnet, the communication protocols, the drive-by download technique for spreading malicious content and the advanced fast-flux service network. The main features of the Asprox botnet are the use of centralized command and control structure, HTTP based communication, use of advanced double fast-flux service networks, use of SQL injection attacks for recruiting new bots and social engineering tricks to spread malware binaries. Hydra fast-flux network, use of SQL injection attack tool is advanced features of Asprox. This paper introduced the botnet advanced features such as hydra fast-flux network.

AsSadhan *et al*. [18] discovered a bots by looking for periodic behavior in the Command and Control communication traffic in the monitored network. They extract from a bot's Command and Control communication traffic the packet count sequence to evaluate its periodogram.

Riccardi *et al*. [19] proposed the framework aimed to manage the whole workflow of identifying, analyzing, and mitigating a financial botnet, ranging from an initial malware analysis to the creation of specific feedback and knowledge shared with interested parties cooperating to fight cybercrime. This paper presents a work-in-progress research aimed at creating a system able to mitigate the financial botnet problem. The proposed system is based on a novel architecture that has been validated by one of the biggest savings banks in Spain.

Goel *et al*. [20] focused on a practical host-based methodology to the collect evidentiary information from a Bot-infected machine. They studied on the analysis of BotNet behaviors, propagation, and method to detect and stop their proliferation. There approach collects digital traces from both the network and physical memory of the infected local host, and correlates
the information to identify the resident BotNet malware involved.

Binsalleeh *et al.* [21] focused on reverse engineering results for the Zeus crimeware toolkit, one of the recent and powerful crime ware tools that emerged in the Internet underground community to control botnets. The Zeus crimeware toolkit is an advanced tool used to generate very effective malware that facilitates criminal activities. They have also designed a tool to automat the recovery of the encryption key and the extraction of the configuration information from the binary bot executables. Analyze and extract the Zeus C&C servers use encryption input system.

Flaglien *et al.* [22] proposed on the design framework for discovering and correlating evidence from multiple components in a particular computer. To combine multiple evidence sources, all the data must be represented in the same format. Design a common representation format for evidence from multiple sources. The correlation method supports forensic investigations using link mining techniques.

Stone-Gross *et al.* [3] focused on efforts to control of the Torpig botnet, is large and targets a variety of applications, then gathers a rich and diverse set of data from the infected victims. Analyzing a cyber-warfare scenario, the possibility of taking over botnet control may also be considered to conduct counter-attack actions. They describe their experience in actively seizing control of the Torpig botnet for ten days. Torpig introducing Mebroot only when necessary to understand Totpig's behavior. These primarily focus on the Master Boot Record (MBR) overwriting rootkit technique employed by Mebroot.

Balzarotti *et al.* [23] focused on infection data from major botnets: Conficker, MegaD, and Srizbi. In this analysis, they examine commonly-infected networks which appear to be extremely prone to malware infection. They provide an in-depth passive and active measurement study. They have proposed and verified cross-botnet prediction techniques to predict unknown victims of one botnet from the information of the other botnet if they have similar infection vectors. In future work, they will study new approaches to explain relationships between geopolitical locations and malware infection more clearly with some realistic examples.

## 4. MODEL OF BOTNET FORENSIC

### 4.1 WT-SIR model (SIR based on Web-Trojan)

Yun *et al.* [24] the common propagation and evolution model to study the spreading features of bots but exactly unable to describe how the bots spread on the Internet. This model is used to analyze botnet propagation rules and predict its tendency. This traditional model is also beneficial to get better the efficiency and precision of propagation with extend the survival period of bots itself.

### 4.2 ADSIR model

Li *et al.* [25] ADSIR model based on the difference of propagation capacity of conficker in different time zone and divide each country into different time zone. Conficker is a worm outbreak recently which forms a large botnet and became a huge threat to the internet security. The redirect technology of domain name was used to monitor the conficker. ADSIR model only considers the propagation method based on remote overflow but not includes the sharing method like Shared Directory, e-mail etc which create problems to describe the botnet propagation accurately.

### 4.3 Diurnal (Botnet Propagation Using Time Zones) Model

Dagon *et al.* [26] the diurnal model also lets one compare propagation rates for different botnets, and prioritizes response. Time zones play an important and unexplored role in malware epidemics to understand how time and location affect malware spread dynamics. Time zones play an important role in botnet growth dynamics, and factors such as time-of-release are important to short-term spread rates.

The model uses diurnal shaping functions to capture regional variations in online vulnerable populations. The computers in each time zone have the same diurnal dynamics, no matter whether they are infected or still vulnerable. The diurnal property of computers is observed by computer user behavior, not by the infection position of computers. If a user changes diurnal behavior because of system infection, then assume the system will quickly be patched or removed by the user.

### 4.4 SIS (susceptible-infected-susceptible) model

Wierman *et al.* [27] this is elementary epidemic models which based on how they relate to the problem of modeling the spread of computer viruses. Computer viruses are tremendously important aspect of computer security, and their infection strategy is significant aspect of any defensive strategy. The deterministic SIS model was introduced by Ross (1915).

In this model, susceptible are susceptible to infection from any infected individual. When a susceptible becomes infected (labeled), it is immediately infectious. Upon "treatment", an individual is labeled S and is immediately once again susceptible. Susceptible–Infected–Susceptible (SIS) is a more realistic epidemiological model which includes a reintroduction parameter with continuously discharge of a computer virus, or the introduction of a latest virus.

## 5. BOTNET DEFENSE TECHNIQUES

Defense techniques against bots focused on two main activities: propagation and bot communication. Combating bot/worm spread directly affects the number of compromised machines in a botnet, thus reducing the network power and utility to the botmaster. Conversely, considering already infected machines, another form of defense is to stop the communication between bots and C&C servers.

The two defense approaches mentioned in main areas: prevention, treatment and containment. For the defense to be effective there must be actions performed by users, network administrators, and Internet Service Providers (ISPs). For propagation, the most important features for worm spreading are the number of vulnerable machines, infection duration, and infection rate. Prevention techniques thus aimed to reduce the vulnerable population, limit the worm spread, and reduce the botnet size. Preventive actions are related to secure software development, updated system maintenance, vulnerability removal, antivirus program use, training, and user social economic power. Mechanisms employed in malware control are also effective in combating botnets, but that action alone is not enough to stop these threats. Treatment is related to disinfecting zombies to reduce the number of bots and perform system updates to reduce vulnerable hosts and the worm spread rate.

The main reasons for using containment and blocking strategies include the following: Blocking can be automated after bot detection, without depending on human action. These strategies may be implemented directly on the network without an overall solution to all hosts on the Internet. Containment mechanisms must be considered in three aspects as follows: Detection and reaction time, Strategy used to identify and contain Solution topology and scope.

Two techniques were used to gather such information:

mwcollectd developed a software, honeypot [28]. The honeypots compromised and joined a botnet. Behaving as normal bots in the botnet, these honey pot spies provide valuable information about the monitored botnet activities. The software was designed to be infected and automate the information gathering tasks. It acts like a low-interact-tive honeypot, emulating services and vulnerabilities. Such emulations increase the likelihood that the botmaster would realize that it is a monitoring device and evade the system. After botnet infiltration, the authors propose a way to turn the botnet off, changing the DNS server configuration. If the name resolution is redirected to private addresses, bots could not connect to the C&C server anymore, and the botnet itself would be disarticulated. This approach requires the cooperation of the DNS provider. With the involvement of the DNS provider, one may also take control of the entire network by simply configuring a C&C server.

Botnet defences can be organized by phase (Avoidance, detection, and reply) and by role (agent or target).

**TABLE 1: BOTNET DEFENSE**

| Avoidance | | Detection | | Reply | |
|---|---|---|---|---|---|
| Possible Agent | Possible Target | Agent Action | Target Action | Agent Response | Target Response |
| 1.Remote users Protection<br><br>2.Execute & observe perimeter security<br><br>3.Apply e-mail handling security<br><br>4.System maintenance<br><br>5.Users education | Establishing Distributed denial of service defenses as appropriate (traffic filtering, multiple internet connection, IP switching ability,) | 1. Botnet network is observe for system behavior<br><br>2.Monitor transfers suspect email file and IDs systems<br><br>3.Anomalous activity is discuss on traffic profiles | 1. Apply regular Detection technique<br><br>2. Defined a distributed source. | 1. A trap and trace system is separated.<br><br>2. Judge must be strict for preserving evidence<br><br>3. Preserve the data and relevant system locks (firewalls, mail servers, IDs, DHCP Server, Webproxy locks etc.)<br><br>4. Disconnect the network. | 1. Try filtering if small set of source IPs are detected.<br><br>2. Change the target's IP address and black whole the attack traffic upstream<br><br>3.when attacks, apply following strategy:<br><br>a) Identify the attack traffic and block it upstream.<br><br>b) Add bandwidth (depends on the attack size)<br><br>c) Supply only significant services<br><br>d) User rate-limiting |

## 6. RESEARCH CHALLENGES

### 6.1 Collection and Detection:

The first step in Botnet forensic analysis involves collection of bots and detection of attacks. Routinely hackers develop new bots (Grum, TDL-4) which challenges detection of bots.
The bots involve IDS and firewall logs, logs generated by network services and applications, packet captures. A data process will be sufficient for discovery of malicious behavior and a full capture is required for reconstruction of attack behavior. A botnet is an army of compromised machines, also
known as zombies, that are under the command and control of a single botmaster.

### 6.2 Botnet Size:

Waledac Botnet size estimation is difficult because botnet itself was capable of sending about 1.5 billion spam messages a day, or about 1% of the total global spam volume. It will be difficult to operate on a new botnet, especially on the encrypted botnet.

### 6.3 Analysis:

Passive anomaly analysisis usually independent of the traffic content and has the potential to find different types of botnets (e.g., HTTP, IRC and P2P). This approach is, however, limited to a specific botnet structure (e.g.centralized only).
Honeypot due to the difficulty in setup and the active analysis required, the value of honeypots on large-scale networks is rather limited.

### 6.4 Investigation:

The investigation must enable attribution of an attack to a host or a network. The results must meet the admissibility criteria in a court of law. Investigate robust botnet unwanted traffic detection algorithms and how to filter botnet command and control (C&C) traffic early.

### 6.5 Temporal Correlation Technique :

This technique utilize between DNS queries and entropy-based correlation between domain names, for speedier detection. It is difficult to applied a more system level logs such as Process/service executions, memory/CPU utilization,
disk reads/writes. It is a biggest challenges server failure based DNS failures, or failures related to the name servers, as a means for detecting botnets which exhibit double fast flux.

### 6.6 Cryptography :

Asprox botnet does not suitable strong for Cryptography .In the botnet architecture, authenticity and integrity of the bot commands is important.

### 6.7 Reverse Engineering:

Reverse engineering methods can only recover the format of plain text. One gap in recovering the format of encrypted message is how to recover the plain - text message from the cipher-text message.

### 6.8 Complexity:

The major challenges of binary analysis are binary code is complex. Binary analysis needs to the model this complexity accurately in order for the analysis to be accurate.

## 7. CONCLUSION AND FUTURE WORK

The main problem of the botnet system infection that non technical person is not be alert of this malware infection. So this infection direct influence the daily humans life. On the other hand hackers take the unwanted profit of this infection.
The BotNets can include viruses, Trojan backdoors and remote controls, hacker tools such as tools to hide from the operating system, as well as non malicious tools that are useful. The botherder remotely access the botclient and perfume its malicious

operation without the knowledge of victim (botclient). Bot clients follow certain common steps that will help both investigators and researchers in finding ways to discover, defend against, and reduce the threat of botnet technology. Similarly, studying the reasons behind each of the botnet payload can reveal strategy and tactics that can be used against the problem. Particularly, finding ways to reduce the demand element could result in less use of botnets in whole classes of behavior.

Future work is related to comprehensive analysis of cooperation effectiveness of various attack and defense teams and inter-team interaction, the implementation of adaptation and self-learning defence to protect against manipulation by attackers, the expansion of attack and defence library, and the investigation of new defence mechanisms. The important part of future research is providing numerous experiments to study the effectiveness of prospective defence mechanisms against botnets.

## 8. REFERENCES

[1] R. Borgaonkar, "An Analysis of the Asprox Botnet," in Fourth International Conference on Emerging Security Information Systems and Technologies (SECURWARE), 2010., pp. 148-153.

[2] Y. Zeng, X. Hu, and K. G. Shin, "Detection of botnets using combined host-and network-level information," in International Conference on Dependable Systems and Networks (DSN), IEEE/IFIP , 2010 pp. 291-300.

[3] S.-G. Brett, C. Marco, C. Lorenzo, G. Bob, S. Martin, K. Richard, K. Christopher, and V. Giovanni, "Your botnet is my botnet: analysis of a botnet takeover," in Proceedings of the 16th ACM conference on Computer and communications security Chicago, Illinois, USA: ACM, 2009.

[4] L. Wei, M. Tavallaee, G. Rammidi, and A. A. Ghorbani, "BotCop: An Online Botnet Traffic Classifier," in *Seventh Annual, Communication Networks and Services Research Conference, CNSR '09*. 2009, pp. 70-77.

[5] M.Egele, T. Scholte, E. Kirda, and C. Kruegel, "A survey on automated dynamic malware-analysis techniques and tools," *ACM Computing Surveys (CSUR)*, vol. 44, p. 6.

[6] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," *Digital Investigation*, vol. 7, pp. 14-27, 2010.

[7] S. r. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, "Botnets: A survey," *Computer Networks*, 2012.

[8] M. Bailey, E. Cooke, F. Jahanian, X. Yunjing, and M. Karir, "A Survey of Botnet Technology and Defenses," in *Conference For Homeland Security,CATCH '09. Cybersecurity Applications & Technology*, 2009, pp. 299-304.

[9] J. Dae-il, K. Minsoo, J. Hyun-chul, and N. Bong-Nam, "Analysis of HTTP2P botnet: case study waledac," in *IEEE 9th Malaysia International Conference on Communications (MICC)*, 2009, pp. 409-412.

[10] S. Saad, I. Traore, A. Ghorbani, B. Sayed, D. Zhao, L. Wei, J. Felix, and P. Hakimian, "Detecting P2P botnets through network behavior analysis and machine learning," in *Ninth Annual International Conference on Privacy, Security and Trust (PST), 2011*, pp. 174-180.

[11] D. Dong, Y. Wu, L. He, G. Huang, and G. Wu, "Deep analysis of intending peer-to-peer botnet," in *Seventh International Conference on Grid and Cooperative Computing, 2008. GCC'08.*, pp. 407-411.

[12] W. Ping, S. Sparks, and C. C. Zou, "An Advanced Hybrid Peer-to-Peer Botnet," *Dependable and Secure Computing, IEEE Transactions on*, vol. 7, pp. 113-127.

[13] Y. Kugisaki,Y. Kasahara, Y. Hori, and K. Sakurai, "Bot Detection Based on Traffic Analysis," in *International Conference on Intelligent Pervasive Computing, IPC* 2007, pp. 303-306.

[14] M. M. Masud, T. Al-khateeb, L. Khan, B. Thuraisingham, and K. W. Hamlen, "Flow-based identification of Botnet traffic by mining multiple log files," in *First International Conference on Distributed Framework and Applications, DFmA*, 2008, pp. 200-206.

[15] P. Kalakota and C. T. Huang, "On the benefits of early filtering of botnet unwanted traffic," in *Proceedings of 18th Internatonal Conference on, Computer Communications and Networks, ICCCN 2009.*, pp. 1-6.

[16] X.-n. Li, Y. Liu, and H. Zheng, "Peer-to-Peer botnets: Analysis and defense," in *IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, 2009, pp. 140-143.

[17] M. Essaaidi, M. Malgeri, C. Badica, I. Kotenko, A. Konovalov, and A. Shorov, "Simulation of Botnets: Agent-Based Approach," in *Intelligent Distributed Computing IV*. vol. 315: Springer Berlin Heidelberg, 2010, pp. 247-252.

[18] B. AsSadhan, J. M. F. Moura, and D. Lapsley, "Periodic Behavior in Botnet Command and Control Channels Traffic," in *Global Telecommunications Conference On GLOBECOM IEEE*, 2009, pp. 1-6.

[19] M. Riccardi, D. Oro, J. Luna M. Cremonini, and M. Vilanova, "A framework for financial botnet analysis," in *Crime Researchers Summit (eCrime)*, 2010, pp. 1-7.

[20] S. Goel, F. W. Law, K. P. Chow, P. Y. Lai, and H. S. Tse, "A Host-Based Approach to BotNet Investigation?," in *Digital Forensics and Cyber Crime*. vol. 31: Springer Berlin Heidelberg, 2010, pp. 161-170.

[21] H. Binsalleeh, T. Ormerod, A. Boukhtouta, P. Sinha, A. Youssef, M. Debbabi, and L. Wang, "On the analysis of the Zeus botnet crimeware toolkit," in *Eighth Annual International Conference on Privacy Security and Trust (PST), 2010*, pp. 31-38.

[22] K. F. a. A. A. Anders Flaglien, "Identifying Malware Using Cross-Evidence Correlation," *Advances in Digital Forensics*, vol. VII, pp. 169-182, 2011.

[23] R. Sommer, D. Balzarotti, G. Maier, S. Shin, R. Lin, and G. Gu, "Cross-Analysis of Botnet Victims: New Insights and Implications," in *Recent Advances in Intrusion Detection*. vol. 6961: Springer Berlin Heidelberg, 2011, pp. 242-261.

[24] Y. Yun, N. Wei, H. Gu-Yu, and L. Hua-Bo, "A Botnet Passiv Propagation and Evolution Model," in *Second International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC)*, IEEE 2012 pp. 71-74.

[25] R. Li, L. Gan, and Y. Jia, "Propagation model for botnet based on conficker monitoring," in *Second International Symposium on Information Science and Engineering (ISISE), 2009*, 2009, pp. 185-190.

[26] D. Dagon, C. Zou, and W. Lee, "Modeling botnet propagation using time zones," in *Proceedings of the 13th annual network and distributed system security symposium (NDSSâ€™06)*, 2006.

[27] J. C. Wierman and D. J. Marchette, "Modeling computer virus prevalence with a susceptible-infected-susceptible model with reintroduction," *Computational Statistics & Data Analysis*, vol. 45, pp. 3-23, 2004.

[28] S. Vimercati, P. Syverson, D. Gollmann, F. Freiling, T. Holz, and G. Wicherski, "Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks," in *Computer Security â€“ESORICS,*vol. 3679: Springer Berlin Heidelberg, 2005, pp. 319-335.