Macrothink Institute™

Network Protocols and Algorithms
ISSN 1943-3581
2018, Vol. 10, No. 2

Botnet Forensic: Issues, Challenges and Good Practices

Anchit Bijalwan

Dept. of Electrical & Computer Engineering, Arba Minch University

Arba Minch, Gamo Gofa, Ethiopia

E-mail: anchit.bijalwan@gmail.com

Vijender Kumar Solanki,

Dept of Computer Science & Engineering

CMR Institute of Technology (Autonomous)

Hyderabad, TS, India

E-mail: spesinfo@yahoo.com,

Emmanuel Shubhakar Pilli

Malaviya National Institute of Technology India

Jaipur, Rajasthan, India

E-mail: espilli.cse@mnit.ac.in

Received: February 14, 2018 Accepted: May 31, 2018 Published: June 29, 2018

DOI: 10.5296/npa.v10i2.13144 URL: https://doi.org/10.5296/npa.v10i2.13144

Abstract

Unethical hacking of sites, probing, click frauds, phishing, denial of services attack and many such malicious practices affects the organizational integrity and sovereignty. Such activities are direct attacks on the safety, security and confidentiality of the organization. These activities put organizational privacy at stake. Botnet forensic is utilized to strengthen the security tools by understanding the modus operandi of the attacks. The available observations can be utilized in future also to prevent a potential threat to network security. This paper enlightens the novel summary of previous survey including life cycle, classification, framework, detection, analysis and the challenges for botnet forensics. It gives the framework

for botnet forensics to understand the collection, identification, analysis and post mortem activities in each phase. It refers to various botnet attack and their tendencies to proliferate. It highlights the current research gap in context with researcher's previous contributions.

Keywords: Botnet, malware, botnet forensics, botnet identification, botnet analysis.

1. Introduction

On 19th july 2012, as per BBC News, huge spam botnet (Grum) is taken out by security researcher. A botnet which experts believe sent out 18% of the world's spam email has been shut down. Security company Fireeye and spam tracking service SpamHaus worked with local internet service providers (ISP) to shut down the illegal network. The most popular botnet engross in spam activity are Grum, Bobax, Pushdo, Rustock, Bagale, Mega-D, Maazben, Xarvester, Donbot,Gheg. The previous statistic exhibit 80% of all spam is sent by these ten botnets, they use to send 135 billion spam message a day. This statistics are gradually becoming worse now.

McAfee the general malware threat shows the steady growth, which is grown up rapidly increased from 84 million in 2012 to 128 million in 2013. The new malware increased from 2 million in 2010 to 15 million in 2013. According to McAfee global threat intelligence, Sql injection attacks are most is in US followed by Taiwan, Spain, Venezuela, Germany, Brazil and others. As per security research company (Symantec), top botnet victim are China and US. In 2016 survey shows that US regained largest 23% among all countries hosting the most malicious activity. South Korea dropped from first place to fourth in phishing website ranking, China still hold second place with 9% share of malicious computer activity [1].

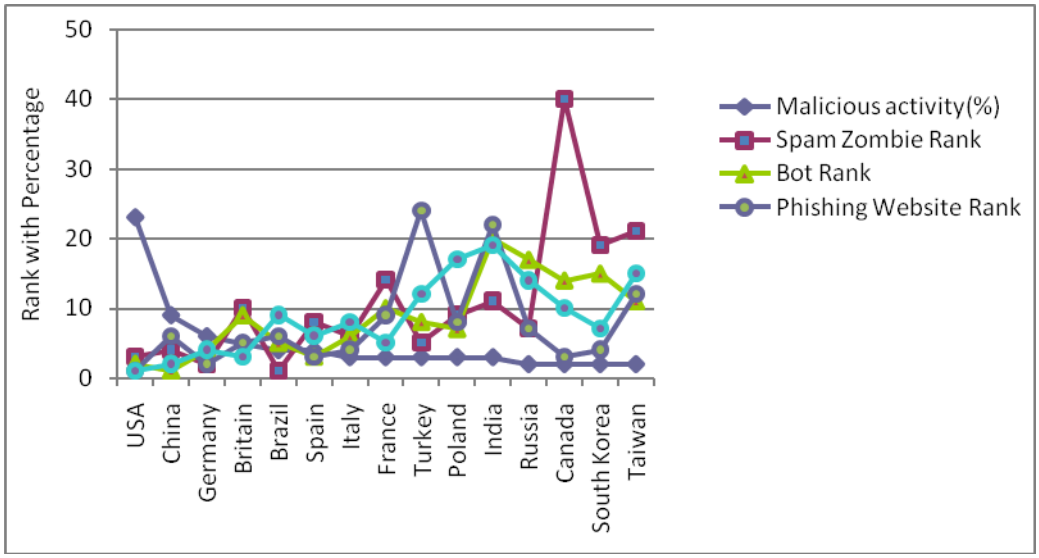

Figure 1.Malicious activity among countries

Figure 1 shows the list of countries in X-axis and the ranking with percentage in Y-axis. This figure includes the malicious activity in percentage, the rank of different countries for spam zombie attack, their bot rank, their phishing website rank and their attack origin rank. If we see separately, ransomware attack embattled India most followed by Russia, Kazakhstan,

Italy, Germany, Vietnam, Algeria, Brazil, Ukraine and US [2] from figure 2. This figure refers to the list of countries in X-axis and their ranking in Y-axis.

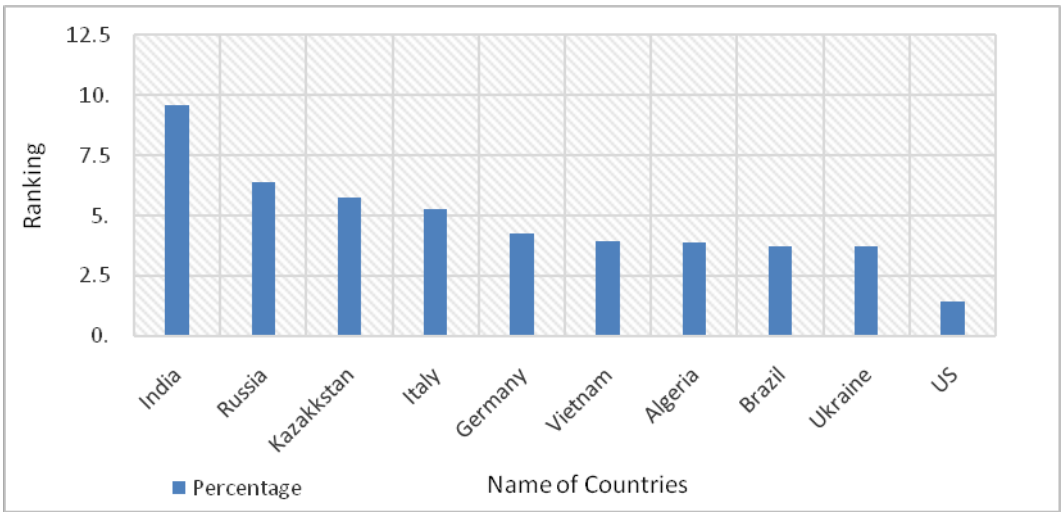

Figure 2. Ransom ware Infected Country

The most distributed denial of service (DDoS) originated country in the world is China followed by US, UK, France, Korea, Singapore, Japan, Vietnam and Germany. Figure 3 shows the most ddos attack originated countries in the world [2]. This figure refers to the list of the countries in X-axis and the percentage of distributed denial of services attack in Y-axis

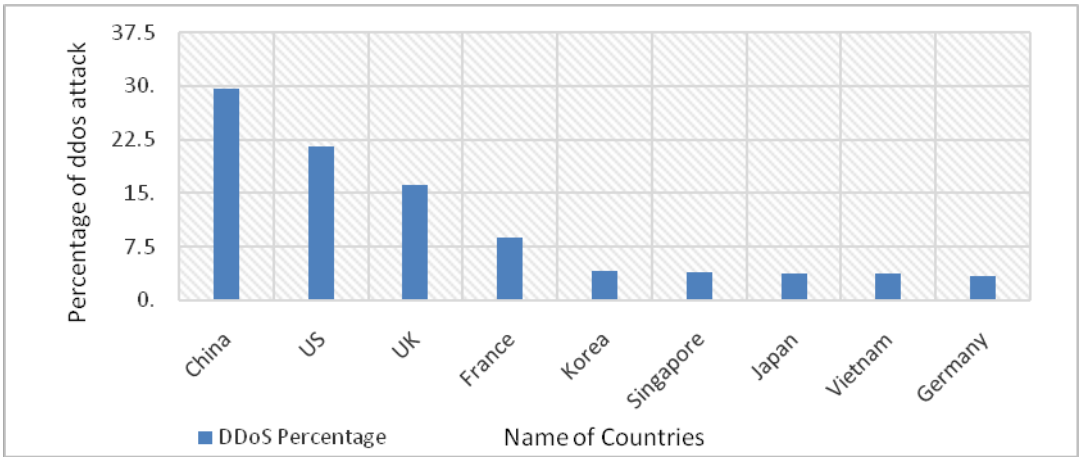

Figure 3. Most DDoS attack originated Country

Botnet forensic deals post mortem activities on botnet attacks and its associated vulnerabilities. Botnet is used for illegal activities such as sending spam, different unwanted emails (Trojan, phishing, spyware, adware, fast flux etc.), media, software, stealing information or computing resource, click fraud, denial of services attacks etc. It is a collection of compromised computer. When a computer is compromised by an attacker, there is often code within the malware (a computer program which is made for harm the system) that commands it to become a part of botnet. It is the most dangerous issue against cyber security as they provided distributed dependencies for many activities. Botmaster or botherder controlled these malicious botnet networks. IRC (inter related chat) network is

specially used by the attacker for managing and controlling the infected hosts because IRC is a most easily available network or server. Bot term came in existence from the word Robot which works as a predefined function or by the software program. it can be directed through command and control channel. Botnets are run by malicious programmer known as botherder or botmmaster. Botherder sends the infection or viruses to the feeble user's computer whose payload is malicious application. It connects through command and control server. Spammer purchase services from the botmaster and botmaster itself issues the updated command.

Botnet forensic is a science which determine the scope of breach and apply the methodology to find out the types of infection. Botnet forensic is the investigation of botnet attacks that includes collection, identification, detection, acquisition and attribution. It is the post mortem activities for the botnet. This paper is the survey of botnet forensics, which categorized botnet investigation into three major categories. These categories are the Framework, Identification and Analysis. The primary contributions of our work are:-

- Novel summary of previous survey.
- Classification of botnet forensics.
- Identification and analysis for botnet forensics.
- Research challenges of botnet forensics.

This paper is organized as follows with section 2 describe the background details of botnet and its survey. Section 3 presents the framework and their gap subsection presents the identification and the Analysis of botnet forensics, section 4 represents its research challenges and Section 5 concludes with future scope the paper.

2. Background of Studies

Botnet forensic is a very young science. The term botnet forensic came in existence after few terminologies such as static forensic, malware forensic and network forensic. Static forensic is the traditional and foundation approach for digital forensics [3, 4]. This analysis is used to identify all deleted file and to determine whether the file is encrypted files or any other. Static forensics obtained clue from identified files that is helpful for previous event results. On the other hand, live forensic deals with those evidence that is not collected by traditional forensics [5]. We can collect all evidence from running system through live forensic. Aquilina et al. [6] explained physical memory is stored on target system from where the evidence can be captured and collected in live forensic [6-8]. Malware forensics is the analysis of malware. It is directly associated with the malicious activity cause by DDoS, phishing, spam, etc. the forensic investigation is needed to get rid of this problem. Figure 4 refers to forensics cycle which consists four phases as start, attack commenced, Investigation undertaken and the Investigation complete.

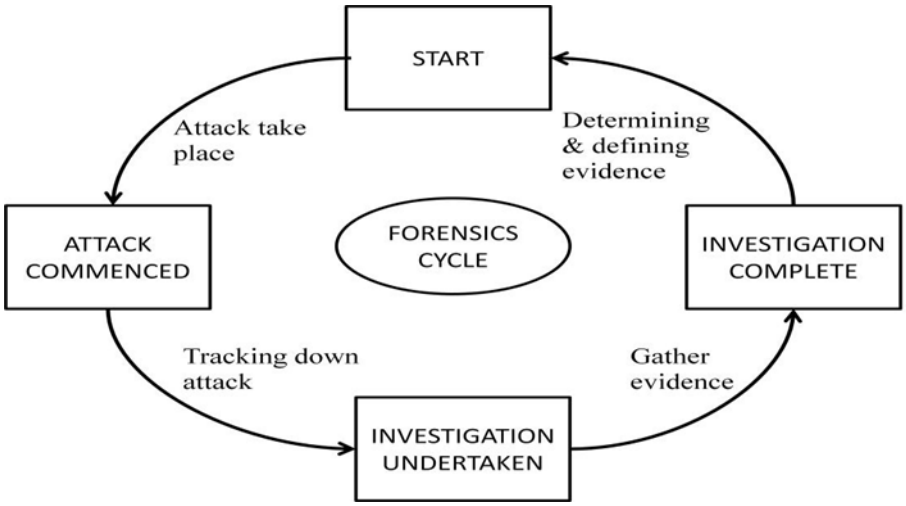

Figure 4: Forensics cycle

In recent times, the network forensics have drawn tremendous significance for ensuring the organization's network security. Network forensics facilitates the detailed analysis of both the outside attacks as well as the insider's abuse. By investigating both kinds of attacks, it ensures its detection of attacks and their prevention in the future, which saves financial loss and the reputation of the organization.

Network security and network forensics are two different technologies. Security products that are utilized for the avoiding intrusion provide data for forensics analysis and investigations. Unlike network forensics, the network security prevents the attack on the system. Network security has a proactive approach as it keeps a close observation on the network and is constantly looking for the abnormal behavior in the context of potential security attack. It is a preventive measure to avoid the malicious activities by the bots. Network forensic is a reactive approach, in which the investigation is usually done after the attack. It is like an autopsy i.e., postmortem investigation. Most often it is observed that it is specific and focused on the type of attack and address only the issues related to the attack.

Ranum coined the term network forensics. Network forensic can be defined as," The reconstruction of network event to provide definitive insight into action and behavior of users, applications as well as devices". However, network forensic is about utilizing the scientific method and tools for collecting, identifying, collaborating, examining, analyzing and to generate the document via using digital information from live network sessions.

Pilli et al. [9] defined the concept of network forensic as "it deals with data found across a network connection mostly ingress and egress traffic from one host to another". He further defined Network forensics as it goes beyond network security as it not only detects the attack, but records the evidence as well. There are certain attacks which do not breach network security policies but may be legally prosecutable. These crimes can be handled only by network forensics. Forensic systems act as a deterrent, as attackers become cautious. They spend more time and energy to cover the tracks in order to avoid prosecution. The Network Forensics is a scientifically proven technique for collecting, identifying, examining, fusing,

analyzing and documenting the all evidences for the purpose of revealing the facts [10].

Giura et al. [11] designed Netstore to store very large amount of network flow data and analyzed them. This system is useful in such cases where the suspects host's all activities keepwatch. Garfinkel et al. [12] classified the network forensics systems into two categories: catch-it-as-you-can tools, stop-look-and-listen tools. Catch-it-as-you-can tools are utilized for capturing all the packets, which passes through a specific traffic point and write them to the storage. This method demands huge amount of storage as the analysis is done in the batch mode. Stop-look-and-listen tools, each packet are analyzed in a minimal required way and only important part is stored in the memory for the future reference. For this approach, a faster processor is required. In both the tools a large amount of storage is required and in both the cases, the tools keep updating itself by erasing the old data so that space can be made for new information.

Sitaraman et al. [13] also classified the network forensics tools into host based tools and network wide tools. Host-based network forensic tools are attacked to a single host in the network. These tools capture all the packets passing through the host and analyze them. Whereas in the case of network-wide forensic, the tools can be utilized for multipoint surveillance on the network by installing tools at different points on the network. This tools facilitates a comprehensive view of the network activity. Niksun and Net detector are the widely and commonly utilized network wide forensic tools.

2.1 Definition

Botnet forensic involves capturing (fetching) the network traffic, retrieving the evidence after reconnaissance from multiple devices, systems, processes and other resources. The information given by botnet forensic is utilized to strengthen the security tools by understanding the modus operandi of the attacks. The available observations can be utilized in future also to prevent a potential threat to network security. Botnet Forensic can be said that it is both the proactive and reactive approach. It not only ensures the network security but also facilitates the law enforcement. The prime objective of botnet forensic is to measure the level of intrusions, investigating them and providing information to recover from an intrusion so as to strengthen system security and retrievable evidence presentation.

Botnet forensic is the science of mitigating, characterizing, trace backing investigating and identifying the clues of bot. Botnet forensics is the technique that assist to ameliorate the system through an analysis of the Bot attack and detecting them. It focuses on the preservation and acquisition of the digital evidence from the various sources to be used as a bot clues for the investigation. Botnet forensics is of great importance now-a-days, as it assists and prevent the organization from the outside and the inside network attacks. It helps to detect the attack and to mitigate the damage occurred by determining who is responsible for an attack and also can determine the path from an affected network or system to the point from where an attack is originated. Table 1 refers to the major botnet and their establishment.

Table 1. Major Botnets and their Establishment

Types of protocol	Bot Name	Discovered	Propagation Mechanism
HTTP	Rusktock	2006	Propagation through spam and infection.
HTTP	Blackenergy	2007	Propagation through infection.
HTTP	Zues	2007	Propagation by downloads.
HTTP	Waledac	2007	Propagation through spam
HTTP	Koobface	2008	Propagation through social networking sites.
HTTP	Lethic	2008	Worm, virus Propagation through spam.
HTTP	Mirai	2016	Targets on consumer devices through scanning.
IRC	GTbot	2000	Involvement for UDP/SYN flood
IRC	Sdbot	2002	Involvement for UDP/ICMP flood.
IRC	Gaobot(Agobot)	2002	Involvement for dos, spam, brute force attack
IRC	Rbot	2003	Involvement for DDoS attack.
IRC	Spybot	2003	Involvement for spam, file deletion and UDP flooding.
IRC	MaXiTE	2003	500 to 1000 server bot. TCL script
IRC	Phatbot	2004	Involvement for DDoS attack, spamming and sniffing traffic
IRC	Mytob	2005	Propagation through email attachment extension.
IRC	Dorkbot	2011	
P2P	Slapper	2002	Involvement in DDoS, spamming and harvest email account.
P2P	Sinit	2003	Installed in OS, exploit the browser and redirect the website.
P2P	Nugache	2006	Involvement in DDoS attack using decentralized custom protocol
P2P	Peacomm	2007	Spamming, DDoS, disable the firewall and attach with mail.
P2P	Conficker	2009	Spamming, through dictionary attack stealing data.
P2P	Kelihos	2010	Spamming, DDoS and embed links through hidden social networking.
P2P	Necurs	2016	Distributor of many piece of malware. Email attachment with javascripts or through macros.

2.2 Classification of Botnet Forensics System

Many researchers contributed their work for botnet. Bailey et al. [14] proposed propagation & compromise, command &Control, Attacks &Theft problems. On the basis of population size, propagation speed, detectability, he explained the different propagation methodology in propagation mechanism. Karasaridis et al. [15] framed the design to

measure the gap between monitored flow data and by default IRC traffic flow.

Wurzinger et al. [16] used regular expression to represent sets of suspicious IRC nick name. He used n-gram analysis to evaluate the nick name for determining the particular conversation hinge upon infected host. Brodsky relied on the same assumption that botnet tend to forward huge no. of spam in a relatively small time period for detecting spam botnet. Zhu et al. [17] surveyed into many areas of botnet including bot anatomy, botnet prediction, honeynet and traffic monitoring. Zhuang et al. [18] worked on Size estimation, gianveccho et al. [19] worked on Behavior analysis, grizzard et al. [20], kanich et al. [21] worked on peer to peer botnet.

Feily et al. [22] segregated botnet detection technique into four classes i.e. signature, anomaly, DNS and mining. He described the botnet phenomenon, botnet characteristics and botnet life cycle. Their botnet detection comparison shows a. The signature based technique can only detect known botnet whereas the other classes detect unknown botnet, b. DNS based technique allow real time detection. DNS uses DNSBL counter intelligence to detect survey in real time however, active countermeasure run the risk of false positives, c. both Mining based and DNS based detection approach effective to detect encrypted C&C botnet communication. Garcia et al. [23] analyze and compare network based detection area. He proposed new dimension to analyze their classification scheme.

Konovalov et al. [24] proposed the simulation based study on investigation of botnet and shared the simulated environment of the various stages of botnet life cycle and efficiency of the correspondent defense mechanism. Lashkari et al. [25] surveyed on their previous paper and introduced different attribute of botnet. He surveyed on botnet protocol specific to IRC, P2P and HTTP.

Broadly we can classify the whole research as following manner and shown in Figure 5.

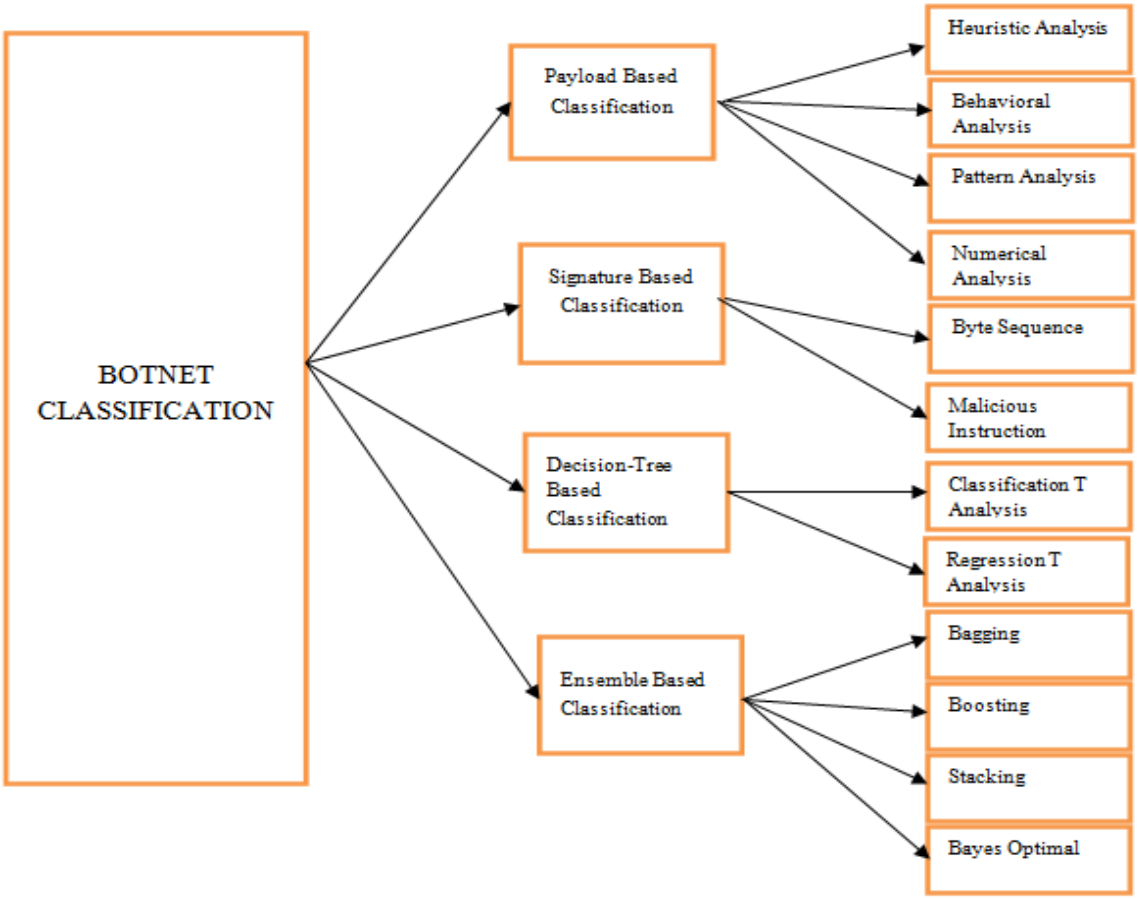

Figure 5. Botnet Forensics Classification

2.2.1 Payload Classification

In payload based traffic classification, packets are classified in the field of the payload. Payload uses classification techniques like Deep Packet Inspection for verification and classification of traffic. For understanding and verifying various applications, Deep packet inspection (DPI) utilizes the signature analysis. In most of the applications unique pattern of signatures exists. There are different signature analysis methods such as pattern analysis, protocol analysis, heuristics analysis, numerical analysis, behavioral analysis.

In Pattern analysis applications have some pattern in the payload of the packets, which can be used to identify the protocols. These patterns may be presented in any position in the packet after this only the classification is possible. Numerical analysis includes the numerical characteristics of the packet for example payload size, the number of response packets, etc. Behavioral analysis and heuristic analysis go simultaneously, and several antiviruses utilizes both techniques for identifying viruses and infections. Protocol analysis, protocols are the set of rules of a particular action.

Lu et al. [26] describes traffic classification as early common techniques which based on the particular port number of a particular protocol to find the network application. It was proved ineffective for these port number based traffic classifications because of the some reasons like new growth of peer to peer network application, the dynamic port number for

some applications, or wrapping different services into the particular application. By utilizing previous work on the application of machine learning algorithm for classification and clustering the traffic flows having a particular set of statistical features [27, 28], a payload content signature model for application traffic classification [29,30] and traffic identification depending on heuristics derived from host communication pattern analysis [31,32] . He tried to detect the P2P traffic rather than particular P2P application. Shortage of sharable dataset and inappropriate metrics became the main cause why the comparison between the mentioned methods failed [33].

2.2.2 Signature Based Classification

The main objective of the signature based classifier is to detect, investigate the nature and find out the feature of a bit string operating in the given payload. There are so many applications that uses primary protocol like in tcp protocol three way handshaking. This classifier is utilized on fredezone, a free network service provider (Wi-Fi) operated by the city of Fredericton Shafi et al. [34] also reconnaissance on the theoretical bounds for learning signatures using existing theory shows a framework for online extraction of signatures using a supervised classifier system.

2.2.3 Decision Tree Based Classification

Decision tree based classification is structure looks like a tree. In this by splitting the dataset into smaller subsets, the decision tree also developed simultaneously, and the outcome is presented in the form of a tree which has decision nodes and leaf nodes. It is a better method of classifying the unknown traffic. It can be further utilized for classification of traffic by initiating from roots of the tree and moving upto complete classification till the leaf node [35] that defines a simple and efficient model for classification of the unknown application into different categories.

2.2.4 Ensemble Based Classification

Livadas et al. [36] identified the Botnet traffic using machine learning technique. For this purpose he segregated the whole traffic into IRC and non IRC traffic. After segregation he differentiated the IRC traffic & real traffic and compare this analysis with J48, naïve Bayes & Bayesian network classifiers. Beigi et al. [37] focuses on statistical network flow features rather than packet content is unable to differentiate between Botnet IRC traffic and benign traffic. Author shows the loophole on previous methods such as principle component analysis (PCA), correlation feature selection (CFS), minimum redundancy maximum relevance (mRMR) and improper evaluation of features set on testbed datasets. He built a dataset which incorporate different variety of botnet of different protocol in realistic environment. Saad et al. [38] proposed a new approach (detecting P2P bot before launch the attack) to characterize and detect through network traffic behavior. Using machine learning technique he extracted, analyzed the set of C&C traffic behavior & its characteristics. He differentiated among five machine learning technique i.e. Super vector machine (SVM), artificial neural network (ANN), nearest neighbors' classifier (NNC), Gaussian based classifier (GBC) and Naïve bayes classifier (NBC). Rokach et al. [39] divided ensemble model into dependent and

independent method. In dependent method the most well versed model instance is boosting which is known as resampling and combining. It is used to improve the performance of week classification on distributed training data. Through iterative process AdaBoost is well known ensemble algorithm to improve simple boosting algorithm. In independent well known method is Bagging and Wagging [40].

2.2 Motivation of Botnet Forensics

Unethical hacking of sites, probing, Click frauds, phishing, denial of services attack and many such malicious practices affects the organizational integrity and sovereignty. Such activities are direct attacks on the safety, security and confidentiality of the organization. These activities put organizational privacy at stake. The main motivation behind this paper is to enlighten on the rapidly increasing number of botnet attacks. Our paper primarily focuses on the different views about botnet, its lifecycle phases and investigates the different attacks. It is basically a survey paper which confides the previous literature on botnet forensic.

3. Botnet Forensic Framework

This section focuses on various proposed framework by the authors. We have categories our work into three phases such as framework, identification and analysis. Farley et al. [41] proposed distributed surveillance intrusion and detection framework. He generated set of controlled attack refer roving bugnet which is used for observing remote distributed controlled system. Bugnet contains compromised system or devices called bugbot. He designed a preliminary mitigation framework that is compatible with most of the windows platform.

Riccardi et al. [42] proposed financial botnet framework based on Dorothy framework and blacklist based IP reputation system. This architecture promote and increased the involvement of low enforcement authorities, financial institution after sharing intelligence information. Zeidanloo et al. [43] proposed and develop detection framework which is based on common pattern and its characteristics of malicious hosts. Wang et al. [44] worked on various existing botnet detection technique in which he analyzed multi sensor information and proposed novel information on fusion model. This model effectively discards the irrelevant information from sensors so that it improved the detection accuracy.

The study proposes a generic framework for botnet forensic based on existing models and researches (Figure 6). The first phase of our generic framework is malware. It is the combination of propagation, infection, communication and attack that shows the stages of malware. As we know botnet has become a common phenomenon on Internet. It is a collection of infected machine or in other word it is a kind of army of infected bots targeted at spreading malicious activity and expansion of bot army. The botmaster controls and communicates through C&C channels. IRC is most commonly and widely utilized channel. This portion shows the kind of malware weather it is botnet or other kind of malware. The second phase of the generic framework is botnet forensic identifier. Our botnet forensic identifier focus on identifying whether the system is compromised or it may get infected. If it

is compromised, it will identify whether it is bot attack or any other kind of attack. Botnet forensic identifier searches the bot through the reconnaissance of traffic, attribution, automotive passive, and malware sample. Our Botnet forensic identifier tries to locate and concentrates on spam email because 80% of email traffic is just because of spam. Botnet forensics identifier also covers the attribution, automotive passive, and malware sample.

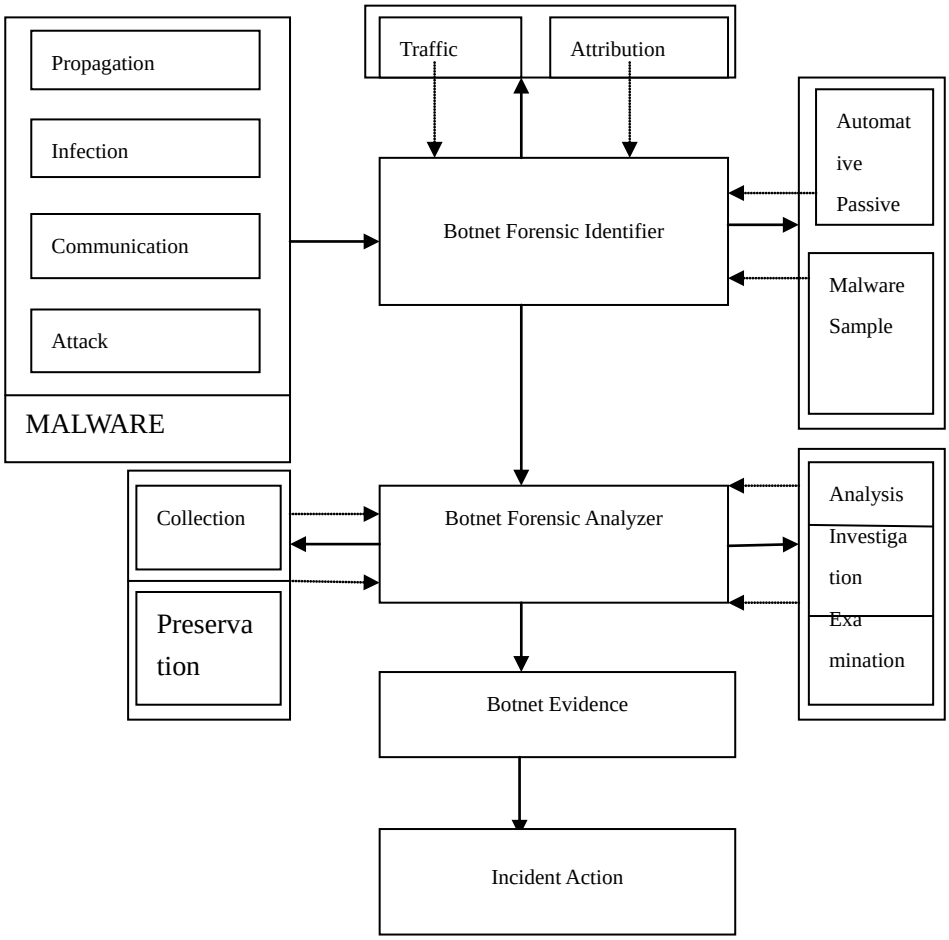

Figure 6. Botnet Forensics Framework

The third phase of the generic framework is Botnet forensic analyzer that analyzes the result generated from the identifier. Botnet forensic analyzer works to search after crime investigation. When identifier insures the malware, analyzer seeks what type of malware it is, where it infected. At this stage analyzer finds out the clues with actual information forward it to botnet evidence phase. It is observedby different phases such as analysis, investigation, examination, collection, and preservation. It includes analysis, investigation, examination, collection, and its preservation. The fourth stage is Botnet evidence that collected all information from the various previous stages and forwards it to incident response phase 3.

3.1 Botnet Forensic Identification

Botnet forensics identification refers to the system involvement in bot malicious activities. This is the initial phase where researcher may get the possibilities of any malicious activities specific to the botnet. Castle et al. [45] showed a novel technique for the automatic

identification of botnets used to deliver malicious email. Author showed a referential implementation system for presenting this technique. This developed system could have deployed in a live environment.

Dacier et al. [46] showed the attack attribution method. This method exhibits some real world result traces in low interaction honeypot. DiBenedetto et al. [47] added the use of TCP fingerprints. He traced the captured spam from ISP's and identified Srizbi botnet. Govil et al. [48] identified the method and types of botnet. Junjie et al. [49] proposed a novel botnet detection system for identifying the stealthy P2P botnets even though it may not be observable. Author's proposal can detect and identify stealthy P2P botnet even when the infected hosts are using legitimate P2P applications and p2p bot software at one time. They proposed high detection accuracy with a low false positive. Using machine learning based classification Livadas et al. [50] identified the compromised host. They compare the performance of J48, Bayesian network and naïve Bayes classifiers that identified the classification accuracy. Van-Hau et al. [51] identified and traced low interaction honeypot belongs to the same botnet without any prior information. He proposed a solution to detect new botnets with very cheap and easily deployable solutions.

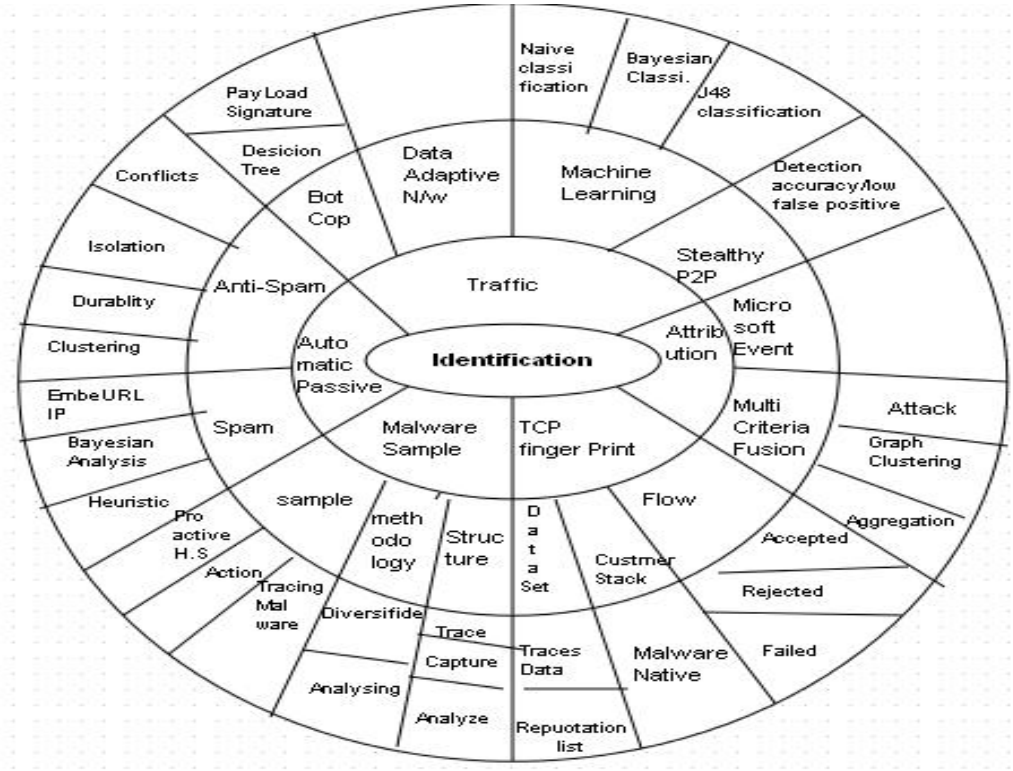

Figure 7. Identification of Botnet Forensics

Wei et al. [52] proposed a new online botnet traffic classification system, named BotCop. Using decision tree model and payload signature author characterize the network traffic flow and analyzed the malicious bot traffic from the normal traffic. They proposed a novel application approach for classifying network applications on a large scale Wi-Fi ISP network. Xiao et al. [53] presented the effective approach to capture malware samples. They designed

and implemented a malware sample capturing and tracking system (MSCTS). This tracking system contains acquisition of unknown malware, information statistics, simulation on network behaviour and automatic analysis. Yu et al. [54] presented the data adaptive technique and showed raw network traffic flows into multi dimensional feature streams and used the correlation analysis. Mohaisen et al. [55] proposed the signature based and behavior based classification technique. He used common sequence of bytes to identify the malware Zeus through classification technique whereas during the execution of these malware artefact created by malware in behavioural based classification. Bijalwan et al. [56] identified the bot clues through random udp flooding.

According to botnet forensic identification Survey, we classified whole identification of botnet forensic process into traffic, attribution, TCP Fingerprint, malware and automotive passive identification (Figure 7).

We classified whole traffic into Bot traffic, Data adaptive network traffic, Machine learning traffic identification. Machine learning traffic identification is classified into naïve classification, Bayesian classification, J48 classification. Automative passive identification classified into spam which include the heuristic, Bayesian analysis and embed url. In anti-spam classification, focuses on isolation, conflicts, clustering and durability. In malware sample shows the sample, proactive heuristic sample, action and tracing malware. Methodology is diversified, analyzing and structure is traced, capture and analyze. In TCP fingerprint identification, we arranged this identification into dataset which show the traces data and the reputation list, customer stack which include the malware native and flow which is accepted, rejected and failed for the identification.

3.2 Botnet Forensic Analysis

Traffic in botnet is an artificial traffic generated from thousand of infected zombies personal computers, i.e. (the computers connected to an infected host and utilized by a bot master to spread malicious activities) some botnet may count more than one million personal computers and aiming among other things at generating fraudulent advertising revenue through click fraud or impression fraud.

Network traffic monitoring refers to keeping a close eye on the traffic movement or inflow or outflow of all the packets on the network and looking for the abnormal behavior and analyzing the traffic behaviors so that the potential threat to network security if any can be detected in it’s advance stages. It protects the efficiency of the networks. The technologies facilitating network traffic monitoring are as follows: Firewalls, Intrusion detection and prevention system, Network monitoring, managing and performance software and, Anti-virus.

The whole analysis is classified into three phases, the Traffic based, IRC based and other analysis. Further traffic based analysis is categorized into five phases, C2 traffic based, P2P based traffic, IRC based traffic, Flow based traffic and DNS based traffic analysis. In others exhibits the cross analysis, host based analysis and malicious probing.

3.2.1 Traffic Based Analysis

3.2.1.1 C2 Traffic Based Analysis

Command & control play an important role in existence of botnet. Masud et al. [57] proposed a temporal correlation technique to detect the command & control bot traffic. They have generated bot clues in log files through TCPdump and exedump. This tool capture the network traffic including all ingress and egress traffic. They extract the related features from log files to detect the command & control bot traffic using data mining techniques.

AsSadhan et al. [58] proposed the periodic behavior of command & control traffic to detect the bot. They focused on period's length effect and duty cycle of the command & control traffic. By test performance they observed and revealed that when duty cycle increase, it also increased and the period length get decreased. They analyzed the performance of test in presence of injected random noise traffic. Tao et al. [59] investigated the bursting characteristics of centralized botnet. Table 2 refers to the traffic analysis.

Table 2. Traffic Analysis

Type	Work	Technique	Tools	Direction	Observation
C&C [57]	Multiple Log File	Temporal correlation Technique	TCPdump/Exedump	Data mining	Detect C2 traffic
C&C [58]	Periodic Behaviour	Walker's Large Sample Test	Tiny P2P generated by SLINGbot	Injected random Noise	C2 traffic to detect bot
C&C [59]	Intrinsic Characteristics	payload& Sequence correlation			similarity & Synchronization among the bot behavior
P2P [60]	Malicious HTTP2P	Waledac as proxibot and workerbot	P2P Over HTTP		Detect the malicious HTTP2P
P2P [61]	P2P protocol		Peacomm based Overnet		Design of advanced P2P
IRC Traffic [62]	Centralised Botnet Detection	IRC Traffic		Behavioral model	Model Distinguish between normal &botnet
Flow [66]	Current network intrusion detection methods	Anamolydetection technique/data mining & visualization		Passive network traffic monitoring	detect malicious traffic via visualization
DNS n/w [65]	Tracking and Analysis	TRAPP-2(Tracking & Analysis for P 2p)	DNS Tunneling	Packet data flow	Detects BitTorrent and Voice over Internet

3.2.1.2 P2P Based Traffic Based Analysis

Dae-il et al. [60] proposed the study of the infected HTTP2P botnet detection. They analyzed on waledac botnet by classifying waledac botnet as proxybot and workerbot.The proposed infected botnet used combination protocol such as HTTP2P i.e. the over HTTP. As this is a combination of both HTTP and P2P, it takes the advantages of both the protocol. This proposed technique detected the infected HTTP2P botnet. Dafan et al. [61] analyzed the difference between normal and advanced P2P protocol for botnet. Bots periodically search the key to get the command for future attack as botherder hardcode the search key in its bot program. Authors designed an advanced hybrid P2P botnet hinge upon the unstructured P2P protocols.

3.2.1.3 IRC Based Traffic Analysis

Mazzariello et al. [62] focused on centralized bot detection. They addressed the known bot always characterized by their propagation mechanism. It may characterized by the next popular.

3.2.1.4 Flow Based Traffic Analysis

Shahrestani et al. [63] analyzed on the current network intrusion detection method. This method based on anomaly detection. It crossed from the flow based detection system for checking worth fullness. Bilge et al. [64] generated the novel technique to overcome the challenges imposed by the analysis of netflow data. After analysis he identified the disclosure to C&C channel traffic using netflow records such as size, temporal behavior and client access pattern.

3.2.1.5 DNS Network Traffic Based Analysis

Thomas et al. [65] analyzed the DNS based botnet detection for P2P version 2. They experimented on extracted DNS based result with the help of hash list size data. Large hash lists results explained the ability to detect traffic under a saturated network load.

3.2.2 IRC Based Analysis

Govil et al. [48] highlighted various detection mechanisms to seek insight into their capability and relevant issues emanating from various perspectives. Author showed botnet infected nature, detection techniques & their IRC client evasion. Kaemarungsi et al. [67] presented the approach to handle the botnet threat using available information from the Shadow server foundation and describe the automate tool. Author presented the statistical data which was captured over two years on botnets. Table 3 refers the IRC based analysis specifically.

Table 3. IRC Based Analysis

Author /Year	Work	Technique	Tools	Direction	Observation
IRC [48]	Detection mechanism/ defense	Honeypot/ Spampot	Nepenthes	DNS Based IDS	More prevention cyber threat
IRC [67]	Handle threat using available information	Incident handling ThaiCERT	Automate tool	Statistical data on botnet threat/ implementation of software script	Installing sensors & monitored tool

3.3 Others

3.3.1 Cross Analysis (Conficker, MegaD, Srizbi)

Shin et al. [68] analyzed the Conficker, MegaD, and Srizbi botnet. They showed cross-analysis uses among conficker, MegaD and Srizbi botnets in order to gain complete knowledge of their infection. In this analysis, author examined common infected networks which is extremely prone to malware infection. Based on cross-analysis results, author derived new implications and insights for defense. They empirically showed the historic infection data of some known botnet that uses the same infection type with more than 80% accuracy. Jungsuk et al. [69] showed cross analysis among 10 spamming botnet to analyze malware infected host.

Table 4. Others

Type	Work	Technique	Tools	Direction	Observation
Cross analysis [69]	Infected data	Cross analysis among them	Conficker, MegaD,Srizbi	Prone to malware infection	Fine grained infection information & nature
spam [70]	Zombie host based analysis	Distinguishes legitimate mail & Spam	Mail Transfer Agent(MTA)	E-mail parameter	Email filtering, n/w delay, Avoid high false rate
Malicious Probe [71]	Malicious probing traffic	Monitored by sensor	Honeynet/ DShield	Scaning events	Information for probing activity

3.3.2 Host Based Analysis

Wang et al. [70] proposed a method to detect zombie hosts. They proposed a method to modify filtering process on firewall layer. They differentiated mail as non spam and spam from

the external parameter. This technique increased the speed of filtering the mail and reduced the network delay. This process neglects the problem of high false rate.

3.3.3 Malicious Probing Analysis

Zhichun et al. [71] analyzed the malicious probing traffic in order to find out the significance of large-scale "botnet probes". In this process, the collection of remote hosts observed by a sensor in coordinated fashion. They designed schemes to extrapolate the global properties of scanning events.

4. Research Challenges

The exhaustive work covered the investigation on botnet forensics designed by different authors. There were some limitations in different phases however this section enlights the gap require in each phase. The exhaustive survey finds research gaps in following phases:

4.1 Collection Phase

- Effective mechanism is to be in place to identify attack features from packet captures.
- Capturing the bot traffic in real time, transmitted through high speed network.

4.2 Identification Phase

- Attacks must be identified instantaneously to trigger forensics process.
- Type of attack must be identified. It should be possible in real time.
- Traces must be stored of identified network
- The network events which are malicious must be identified.
- unauthorized events and anomalies can be identified through real time identification
- The flow based temporal correlation utilizes two different log files whereas, it may be applied on more system level logs such as those that track process, service execution, memory, cpu utilization, disk reads or write and so on. Using this approach a real time C&C traffic detection system can be implemented.
- Efficient technique to detect the centralize botnet.

4.3 Analysis Phase

- Attack information and alerts must be taken from various security sensors as no single security tool can give comprehensive alert information.
- Information must be considered from various hosts from a compromised network for reconnaissance.
- Chances of improvement of data accuracy.
- Waledac traffic is similar to P2P traffic. It is hard to detect a traffic flow. It is still challenges to apply this into flow based detection.
- The deep analysis on IRC traffic is still the challenge.
- Machine learning technique required to improve the algorithm.

5. Conclusion and Future Scope

Botnet Forensic is a proactive and reactive investigation on Botnet. However this study is based on prior research reactive investigation. Our survey shows the framework of botnet forensic which include the Identification and an analysis. We surveyed the prior researcher work and implement the generic framework of Botnet Forensic. This paper focuses on the different views of botnet and its life cycle phases and investigates the different attacks. We made an extensive survey on various botnet forensic and develop the botnet forensic framework model. Many researchers examined the botnet with some technique but not specifically towards botnet forensic. This survey paper identify the serious problem of botnet specific in forensics, analyze the recent research work, prepare a framework on botnet forensic works and it results then finally research challenges on botnet forensic. This paper enlighten on botnet and its related activity from beginning to the ends. From different sections, we observed some research gap which we have covered in our research and challenges section.

The study is an attempt for reconciliation of the research gap. It endeavors the work for the future in the line with mitigating the probability of severe bot attacks. This work can be implemented through different machine learning algorithm either single or ensemble based machine learning. This work can be achieved through high performance computing.

References

[1] Available at: http://www.cybersecurity-insiders.com/ [Last Access: May 31, 2018]

[2] Available at: https://www.enigmasoftware.com/ [Last Access: May 31, 2018]

[3] Adelstein, F., "Live forensics: diagnosing your system without killing it first". Communication of the ACM, Vol. 49, no.2, pp. 63-66. 2006. https:// doi.org/10.1145/1113034.1113070

[4] Hay, B.; Bishop,M.; and Nance, K.," Live analysis: Progress and challenges". Security & Privacy, IEEE, vol. 7, no. 2, pp. 30-37. 2009. https://doi.org/10.1109/MSP.2009.43

[5] Aquilina, J.M.," Chapter 6-Legal Considerations". Malware Forensics Burlington: Syngress, pp. 253-281. 2008.

[6] Dhinakaran, C. and Lee, J.K.," An empirical study of spam and spam vulnerable email accounts". Future generation communication and networking (fgcn). vol. 1 Jeju: IEEE, pp. 408-413. 2007. https:// doi.org/10.1109/FGCN.2007.61

[7] Deng, J.; Xia, H.; Fu, Y.; Zhou, J. and Xia, Q.," Intelligent spam filtering for massive short message stream". COMPEL-The international journal for computation and mathematics in electrical and electronic engineering, vol. 32, no. 2, pp. 586-596.2013. https:// doi.org/abs/10.1108/03321641311296963

[8] Govil, J.," Examining the criminology of bot zoo". 6th International Conference on Information, Communications & Signal Processing, 2007 Singapore, pp. 1-6. 2007. https:// doi.org/10.1109/ICICS.2007.64449633

[9] Pilli, E.S.; Joshi, R.C. and Niyogi, R.," Network forensic frameworks: Survey and research challenges". Digital investigation, vol. 7, no. 1, pp. 14-27. 2010. https:// doi.org/10.1016/j.din.2010.02.003

[10] Palmer, G.L.," Forensic analysis in the digital world". International Journal of Digital Evidence, vol. 1, no. 1, pp. 1-6. 2009.

[11] Giura, P.; Memon, N; Jha, S.; Sommer,R.; and Kreibich, C.," NetStore: An Efficient Storage Infrastructure for Network Forensics and Monitoring Recent Advances in Intrusion Detection". vol. 6307: Springer Berlin / Heidelberg, pp. 277-296. 2010. https://doi.org/10.1007/978-3-642-15512-3_15

[12] Garfinkel, S. and Spafford, G. (2002).Web security, privacy & commerce: " O'Reilly Media, Inc." 2002.

[13] Sitaraman, S. and Venkatesan, S.," Computer and network forensics". Digital Crime and Forensic science in cyberspace. vol. 3, 2006, pp. 55-74. 2006.

[14] M. Bailey, B.; Cooke, E.; Jahanian, F.;Yunjing, X. and Karir, M.," A Survey of Botnet Technology and Defenses" Cybersecurity Applications & Technology Conference For Homeland Security. CATCH '09. Washington, DC, pp. 299-304. 2009. https:/DOI.org/ 10.1109/CATCH.2009.40

[15] Karasaridis, A.; Rexroad, B. and Hoeflin, D.," Wide-scale botnet detection and characterization". First conference on First Workshop on Hot Topics in Understanding Botnets. 2007.

[16] Wurzinger, P.; Bilge, L.; Holz, T.; Goebel, J.; Kruegel, C.; Kirda, E.; Backes, M. and Ning, P.," Automatically Generating Models for Botnet Detection Computer Security". vol. 5789: Springer Berlin / Heidelberg, pp. 232-249. 2009.

[17] Zhu, Z.; Lu, G.; Chen, Y.; Fu, Z.J.; Roberts, P. and Han, K.," Botnet research survey". pp. 967-972. 2008. https:/DOI.org/ 10.1109/COMPSAC.2008.205

[18] Zhuang, L.; Dunagan, J.; Simon, D.R.; Wang, H.J.; Osipkov, I. and Tygar, J.D.," Characterizing Botnets from Email Spam Records". LEET, vol. 8, pp. 1-9, 2008.

[19] Gianvecchio, S.; Xie, M.; Wu, Z. and Wang, H.," Measurement and Classification of Humans and Bots in Internet Chat". USENIX security symposium, pp. 155-170. 2008.

[20] Grizzard, J.B.; Sharma, V.; Nunnery, C.; Kang, B.B and Dagon, D.," Peer-to-peer botnets: Overview and case study". First Workshop on Hot Topics in Understanding Botnets Cambridge, MA, pp. 1-8. 2007.

[21] Kanich, C.; Kreibich, C.; Levchenko, K.; Enright, B.; Voelker, G.M.; Paxson, V.; and Savage, S.," Spam analytics: An empirical analysis of spam marketing conversion". CCS'08 Alexandria, Virginia, USA.: ACM, pp. 3-14. 2008. https:/DOI.org/10.1145/1455770.1455774

[22] Feily,M.; Shahrestani, A. and Ramadass, S.," A survey of botnet and botnet detection". Third International Conference on Emerging Security Information, Systems and Technologies Athens, Glyfada: IEEE, pp. 268-273. 2009. https:/DOI.org/10.1109/SECURWARE.2009.48

[23] Garcia, S.; Zunino, A. and Campo, M.," Survey on network□based botnet detection methods". Security and Communication Networks, vol. 7, no. 5. 2014. https:/DOI.org/full/10.1002/sec.800

[24] Konovalov, A. M.; Kotenko, I.V. and Shorov, A. V.," Simulation-based study of botnets and defense mechanisms against them". Journal of Computer and Systems Sciences International, vol. 52, no. 1, pp. 43-65, 2013. https://doi.org/10.1134/S1064230712060044

[25] Lashkari, A.H.; Ghalebandi, S.G. and Moradhaseli, M.R.," A Wide Survey on Botnet". Digital Information and Communication Technology and Its Applications Dijon, France: Springer, pp. 445-454. 2011. https://doi.org/10.1007/978-3-642-21984-9_38

[26] Lu, W.; Tavallaee, M.; Rammidi, G. and Ghorbani, A.A.," BotCop: An online botnet

traffic classifier". Seventh Annual Communication Networks and Services Research Conference, CNSR '09. Moncton, NB: IEEE, pp. 70-77. 2009. https://doi.org/10.1109/CNSR.2009.21

[27] Erman, J.; Mahanti, A.; Arlitt, Cohen, I. and Williamson, C.," Offline/realtime traffic classification using semi-supervised learning". Performance Evaluation, vol. 64, no. 9, pp. 1194-1213. 2007. https://doi.org/10.1016/j.peva.2007.06.014

[28] Bernaille, L.; Teixeira, R.; Akodkenou, I.; Soule, A. and Salamatian, K.," Traffic classification on the fly". ACM SIGCOMM Computer Communication Review, vol. 36, no. 2, pp. 23-26. 2006.

[29] Bernaille, L. and Teixeira, R.," Early recognition of encrypted applications". in Passive and Active Network Measurement: Springer, pp. 165-175. 2007. https://doi.org/10.1007/978-3-540-71617-4_17

[30] Sen, S. and Wang, J.," Analyzing peer-to-peer traffic across large networks". IEEE/ACM Transactions on Networking (ToN), vol. 12, no. 2, pp. 219-232. 2004. https://doi.org/10.1145/637201.637222

[31] Karagiannis, T.; Papagiannaki, K. and Faloutsos, M.," BLINC: multilevel traffic classification in the dark". ACM SIGCOMM Computer Communication Review, pp. 229-240. 2005. https://doi.org/10.1145/1080091.1080119

[32] Moore, A. W. and Papagiannaki, K.,"Toward the accurate identification of network applications". Passive and Active Network Measurement: Springer, pp. 41-54. 2005. https://doi.org/10.1007/978-3-540-31966-5_4

[33] Salgarelli, L.; Gringoli, F. and Karagiannis, T.," Comparing traffic classifiers". ACM SIGCOMM Computer Communication Review, vol. 37, no. 3, pp. 65-68. 2007. https://doi.org/10.1145/1273445.1273454

[34] Shafi, K. And Abbass, H.A.," Analysis of Online Signature Based Learning Classifier Systems for Noisy Environments: A Feedback Control Theoretic Approach". Simulated Evolution and Learning: Springer, pp. 395-406. 2014. https://doi.org/10.1007/978-3-319-13563-2_34

[35] Rehak, M.; Pechoucek, M.; Grill, M.; Stiborek, J.; Barto, K. and Celeda, P.," Adaptive multiagent system for network traffic monitoring". IEEE Intelligent Systems, no. 3, pp. 16-25. 2009. https://doi.org/10.1109/MIS.2009.42

[36] Livadas, C.; Walsh, R.; Lapsley, D. and Strayer,W. T." Using Machine Learning Technliques to Identify Botnet Traffic". 31st IEEE Conference on Local Computer Networks, Tampa, FL, pp. 967-974. 2006. https://doi.org/10.1109/LCN.2006.322210

[37] Beigi, E.B.; Jazi, H.H.; Stakhanova, N. and Ghorbani, A.A.," Towards effective feature selection in machine learning-based botnet detection approaches". IEEE Conference on Communications and Network Security (CNS), San Francisco, CA: IEEE, pp. 247-255. 2014. https://doi.org/10.1109/CNS.2014.6997492

[38] Saad, S.; Traore, I.; Ghorbani, A.A.; Sayed, B.; Zhao, D.; Lu, W.; Felix, J. And Hakimian, P.," Detecting P2P botnets through network behavior analysis and machine learning". Ninth Annual International Conference on Privacy, Security and Trust (PST), Montreal, QC: IEEE, pp. 174-180. 2011. https://doi.org/10.1109/PST.2011.5971980

[39] Rokach, L.," Ensemble-based classifiers". Artificial Intelligence Review, vol. 33, no. 1-2,

pp. 1-39. 2010. https://doi.org/10.1007/s10462-009-9124-7
[40] Bijalwan A.;Chand N.; Pilli E.S.; Krishna C.R.," Botnet analysis using ensemble classifier". Perspectives in Science. Vol 8, pp. 502-504. 2016. https://doi.org/10.1016/j.pisc.2016.05.008
[41] Farley, R. and Wang, X.," Roving bugnet: Distributed surveillance threat and mitigation," Computers & Security, vol. 29, no. 5, pp. 592-602. 2010. https://doi.org/10.1016/j.cose.2009.12.002
[42] Riccardi, M.; Oro, D.; Luna, J.; Cremonini, M. and Vilanova, M.," A framework for financial botnet analysis". eCrime Researchers Summit (eCrime). Dallas, TX, pp. 1-7. 2010. https://doi.org/10.1109/ecrime.2010.5706697
[43] Zeidanloo, H.R.; Bt Manaf, A.; Vahdani, P.; Tabatabaei, F. and Zamani, M.," Botnet detection based on traffic monitoring". International Conference on Networking and Information Technology (ICNIT), Manil, pp. 97-101. 2010. https://doi.org/10.1109/ICNIT.2010.5508552
[44] Wang, H. And Gong, Z.," Heterogeneous Multi-sensor Information Fusion Model for Botnet Detection". International Conference on Intelligent Computation Technology and Automation (ICICTA), vol. 2 Changsha, pp. 428-431. 2010. https://doi.org/10.1109/ICICTA.2010.575
[45] Castle, I. and Buckley, E.," The Automatic Discovery, Identification and Measurement of Botnets". Second International Conference on Emerging Security Information, Systems and Technologies Cap Esterel, France, pp. 127-132. 2008. https://doi.org/10.1109/SECURWARE.2008.44
[46] Dacier, M.;V.-H. Pham, O. Thonnard, A. Prakash, and Gupta Sen I., "The WOMBAT Attack Attribution Method: Some Results Information Systems Security." vol. 5905: Springer Berlin / Heidelberg, pp. 19-37. 2009.
[47] DiBenedetto, S.; Gadkari, K.; Diel, N.; Steiner, A.; Massey, D. and Papadopoulos, C.," Fingerprinting custom botnet protocol stacks". Secure Network Protocols (NPSec), 6th IEEE Workshop on, pp. 61-66. 2010.
[48] Govil, J. and Jivika, G.," Criminology of BotNets and their detection and defense methods". IEEE International Conference on Electro/Information Technology, Chicago, IL, pp. 215-220. 2007. https://doi.org/10.1109/EIT.2007.4374517
[49] Junjie, Z.; Perdisci, R.; Wenke, L.; Sarfraz, U. and Xiapu, L.," Detecting stealthy P2P botnets using statistical traffic fingerprints". 41st IEEE/IFIP International Conference on Dependable Systems & Networks (DSN), Hong Kong, pp. 121-132. 2011. https://doi.org/10.1109/DSN.2011.5958212
[50] Livadas, C.; Walsh, R.; Lapsley, D. and Strayer, W.T.," Using Machine Learning Technliques to Identify Botnet Traffic". 31st IEEE Conference on Local Computer Networks, Proceedings Tampa, FL, pp. 967-974. 2006. https://doi.org/10.1109/LCN.2006.322210
[51] Pham, V.H. and Dacier, M.," Honeypot trace forensics: The observation viewpoint matters". Future Generation Computer Systems, vol. 27, no. 5, pp. 539-546. 2010. https://doi.org/10.1016/j.future.2010.06.004
[52] Wei, L.; Tavallaee, M.; Rammidi, G. and Ghorbani, A.A.," BotCop: An Online Botnet Traffic Classifier". Seventh Annual Communication Networks and Services Research

Conference, CNSR '09. Moncton, NB, pp. 70-77. 2009. https://doi.org/10.1109/CNSR.2009.21
[53] Xiao, J.; Hao, Z.; Wang, Y.," A Malware Sample Capturing and Tracking System". Second World Congress on Software Engineering (WCSE), vol. 1 Wuhan, pp. 69-72. 2010. https://doi.org/10.1109/WCSE.2010.48
[54] Yu, X.; Dong, X.; Yu, G.; Qin, Y. and Yue, D., "Data-Adaptive Clustering Analysis for Online Botnet Detection". Third International Joint Conference on Computational Science and Optimization (CSO), vol. 1 Huangshan, Anhui, China, pp. 456-460. 2010. https://doi.org/10.1109/CSO.2010.214
[55] Mohaisen, A. and Alrawi, O.," Unveiling Zeus: automated classification of malware samples". 22nd international conference on World Wide Web companion Rio de Janeiro, Brazil: International World Wide Web Conferences Steering Committee, pp. 829-832. 2013. https://doi.org/10.1145/2487788.2488056.
[56] Bijalwan, A; Wazid, M; Pilli,E and Joshi, R.," Forensics of Random- UDP flooding attacks". Journal of Networks. Vol. 10, No. 5. pp. 287-293. 2015.
[57] Masud, M.M.; Al-khateeb, T.; Khan, L.; Thuraisingham, B. and Hamlen, K.W.," Flow-based identification of botnet traffic by mining multiple log files". First International Conference on Distributed Framework and Applications, Penang, pp. 200-206. 2008.
[58] AsSadhan, B.; Moura, J.M.F. and Lapsley, D.," Periodic Behavior in Botnet Command and Control Channels Traffic," in IEEE Global Telecommunications Conference, Honolulu, USA, pp. 1-6. 2009. https://doi.org/10.1109/GLOCOM.2009.5426172
[59] Tao, W. And Shun-Zheng, Y.," Centralized Botnet Detection by Traffic Aggregation". IEEE International Symposium on Parallel and Distributed Processing with Applications, Chengdu, pp. 86-93. 2009. https://doi.org/10.1109/ISPA.2009.74
[60] Dae-il, J.; Minsoo, K.; Hyun-chul, J. and Bong-Nam, N." Analysis of HTTP2P botnet: case study waledac". IEEE 9th Malaysia International Conference on Communications (MICC) Kuala Lumpur, pp. 409-412. 2009. https://doi.org/10.1109/MICC.2009.5431541
[61] Dafan, D.; Ying, W.; Liang, H.; Guowei, H. and Gongyi, W. (2008). Deep Analysis of Intending Peer-to-Peer Botnet. Seventh International Conference on Grid and Cooperative Computing, GCC '08. Shenzhen, pp. 407-411. https://doi.org/10.1109/GCC.2008.51
[62] Mazzariello, C.," IRC Traffic Analysis for Botnet Detection," in Fourth International Conference on Information Assurance and Security, ISIAS '08. Naples, pp. 318-323. 2008. https://doi.org/10.1109/IAS.2008.58
[63] Shahrestani, A.; Feily, M.; Ahmad, R. and Ramadass, S." Architecture for Applying Data Mining and Visualization on Network Flow for Botnet Traffic Detection". International Conference on Computer Technology and Development, ICCTD '09. Kota Kinabalu, Malaysia, pp. 33-37. 2009. https://doi.org/10.1109/ICCTD.2009.82
[64] Bilge, L.B.; Robertson, D.; Kirda, W.; Kruegel, E.; Christopher." Disclosure: detecting botnet command and control servers through large-scale NetFlow analysis". 28th Annual Computer Security Applications Conference orlando, USA: ACM, pp. 129-138. 2012. https://doi.org/10.1145/2420950.2420969
[65] Thomas, B.; Mullins, B.; Peterson, G.; Mills, R. and Shenoi, S." An FPGA System for Detecting Malicious DNS Network Traffic Advances". Digital Forensics VII." vol. 361: Springer Boston, pp. 195-207.2011. https://doi.org/10.1007/978-3-642-24212-0_15

[66] Masud,M.M.; J; Khan, L; Han,J; and Thuraisingham, B.," Integrating Novel Class Detection with Classification for Concept-Drifting Data Streams". Joint European Conference on Machine Learning and Knowledge Discovery in Databases, Berlin, Heidelberg, 2009, pp. 79-94. https://doi.org/10.1007/978-3-642-04174-7_6.

[67] Kaemarungsi, K.; Yoskamtorn, N.; Jirawannakool, K.; Sanglerdsinlapachai, N. and Luangingkasut, C.," Botnet Statistical Analysis Tool for Limited Resource Computer Emergency Response Team". Fifth International Conference on IT Security Incident Management and IT Forensics, IMF '09. Stuttgart, Germany, pp. 27-40.2009. https://doi.org/10.1016/j.comnet.2012.07.021.

[68] Shin, S.; Lin, R. and Gu, G.," Cross-analysis of botnet victims: New insights and implications". Recent Advances in Intrusion Detection, Menlo Park, CA, USA, pp. 242-261.2011. https://doi.org/10.1007/978-3-642-23644-0_13

[69] Song, J,; Shimamura, J.; Eto, M; Inoue, D and Nakao, K," Correlation analysis between spamming botnets and malware infected hosts". in Applications and the Internet (SAINT), 2011 IEEE/IPSJ 11th International Symposium on 2011 Jul 18, pp. 372-375. https://doi.org/10.1109/SAINT.2011.71

[70] Wang, C.D.; Li, T. and Wang, H.B." Botnet Detection Based on Analysis of Mail Flow". 2nd International Conference on Biomedical Engineering and Informatics, BMEI '09. Tianjin, pp. 1-4.2009. https://doi.org/10.1109/BMEI.2009.5305615

[71] Zhichun, L.; Goyal, A.; Yan, C. and Paxson, V.," Towards Situational Awareness of Large-Scale Botnet Probing Events". Information Forensics and Security, IEEE Transactions on, vol. 6, no. 1, pp. 175-188. 2011. https://doi.org/10.1109/TIFS.2010.2086445

Copyright Disclaimer