VOL. 11, NO. 1, JANUARY 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

SURVEY AND BRIEF HISTORY ON MALWARE IN NETWORK SECURITY CASE STUDY: VIRUSES, WORMS AND BOTS

Saif Uldun Mostfa Kamal, Rana Jabbar Abd Ali, Haider Kamal Alani and Esraa Saad Abdulmajed
Faculty of Information Science and Technology, National University of Malaysia (UKM), Malaysia
E-Mail: saifalsamer@yahoo.com

ABSTRACT

Networking provides the main infrastructure for different recent applications. These applications are targets for different types of attack. In this paper a structured literature for different types of attacks has been proposed. It presents a survey of viruses, worms and bots. Latest network security technologies are investigated, the current situation and increasing demand for robust network security is analysed; major portion of network attacks are launched using viruses, worm and bots. One of the most critical attacks are computer viruses. For security specialist it is vital to make difference any reproducing programs, which may not harm your system, and it closer forms. Different researches have been proposed to classify different aspects of metamorphic viruses. Worms is one of the most common propagation attacks over the internet. Two methods can be used by worm to propagate it: finding any vulnerable devices in the network and propagate using topological neighbours. Investigating the methods of worm propagation can provide a clearer vision on how worms propagate and how to defence and prevent such type of attacks. Last decade different mechanisms for detection and defencing have been proposed to deal with the bots attacks. Structures this knowledge can be very critical to better understand the bots behaviour and its detection and defensive approaches.

Keywords: network environment, network security, viruses, worms, propagation, modelling, bots.

INTRODUCTION

Nowadays, with the rapidly development of IT industry, global information has become the major tendency of the development of human society [1]. Information industry has become the pillar industry in the human society and network application is omnipresent [2]. Because of the diversity of the connected types, the uneven distribution of the terminal, as well as the nature of openness and connectivity, the network is easily to be attacked by hacker, viruses, worms, malicious software and other malicious attacks [3]. So virus research has become the popular research subject in network industry. In order to effectively prevent and control computer virus, you must carry on the technical analysis to the virus; understand transmission mechanism and behaviour characteristics of them in computer and the network. They are identified, on this basis it can be prevented and controlled; reduce influence of the virus on the computer and the network. Because the virus has a lot of types, this paper mainly introduces the basic knowledge of the viruses, worms and bots.

Viruses

Viruses carry functions that are intelligent for providing protection in such a manner that detection becomes difficult for virus scanner. Viruses have to take various measures of intellect for survival. That is why they may have complex encrypting and decrypting engines. Encryption and decryption methods are used frequently by virus codes.

Worms

Worms have been a persistent security threat in the Internet since the late 1980s, types of attacks that using worms deny access temporarily to huge parts of internet resources and services. During the past decade, these attacks steal massive amount of financial information causing big losing for investors and financial users which resulted in social disruption. This paper includes the definition of the worm, and its working mechanism, the difference between traditional viruses, behavioural characteristics. Traditional worm and virus is contagious and has the characteristic of replication [4]. It is very difficult to distinguish between them, especially in recent years, more and more traditional virus takes a part of the worm virus technology, on the other hand, destructive worm also took part of technology of the traditional virus [5, 6].

Bots

Bots pose the highest portion of recent network attacks and threats on the internet connected users and applications. Hundreds of scientific researches has been proposed on bots as a result to the rapid rate of botnet attacks and their destructive damages. These researches describe the botnet architecture, behaviour, detection and prevention. Also these researches include the first systematic analysis of the bots threat from three aspects: bots behaviours/architectures, detection mechanisms, and defence strategies.

Malware

Malware is short for malicious software, malware is a specific application or program which is made to disturb or cause damages to users. Malware can be used for different purposes including steal sensitive information, halt computer operation, or acquire access to personal computer system [7]. Malware can hide it identity and survive for long periods of time. During this time it can spy on computer users and steal their information without their knowledge about it existence [7].

The increasing use of internet has made internet a platform for malicious activities. Malicious codes are executable code and have the capability to replicate [8]. It makes their survival strong [9].

Malware cause systems disturbance and damages so it has been considered as one of the top critical users connected to the internet, as the technology developed; there is a continuous conflict between hacker who develops malware and security professional who develop detection and prevention methods. Based on the Symantec Internet security report, in 2009 there were more than 2.89 million different malware were detected. This statistics had increased in 2010 and 2011 to about 286 million and 403 million, which means it has increased to more than 100 times than that before 2009 [10].

Classification of Malware

Malware is classified based on the intent malware designed for. The different most popular malware categories includes viruses , worms, spyware, adware, Trojans and bots as shown in Figure-1 [7].

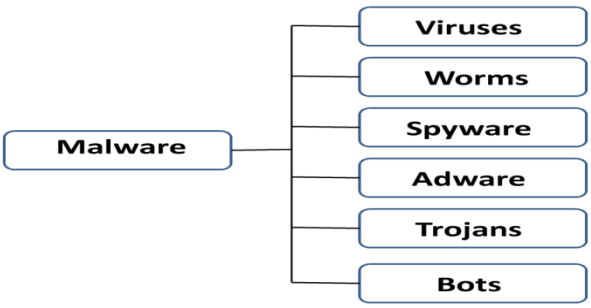

Figure-1. Classification of Malware.

Viruses

Encrypted virus was one of earliest efforts to hide itself from signature based anti-virus software detection. This types of viruses consist of two main parts: the first part which cause the intended damage which is called virus and the other part is a decryption routine which responsible for virus encryption. Encoding the virus part with a new key each time it attaches itself to a user program can change the encrypted virus code structure. The encrypted virus is designed to generate and use variant key for each attack.

Different virus program body can be generated by using variant key for each single process. This new body for each process allow viruses to work in different infection forms, which in turn make it difficult to be detected by the detection mechanism of antivirus. Most of these detection mechanisms depend on searching for the signature of the virus which extracted a constant virus body or binary. On the other hand, latest antivirus software start to look for and detect the virus decryption routine instead of the virus signature, the cause of that change in detection mechanism is that the decryption routines remain unchanged in each virus signature regeneration [7]. Despite that a computer virus is working as a program or piece of code which is activated when it's run without your knowledge and it works to harm your computer. Majority of viruses has the ability to duplicate themselves and propagate through your file system. Viruses in general are coded by humans. Virus design and code allow it to make multiple copies of itself; this process is relatively easy to produce. The target of such dangerous viruses is that it will use all the available memory and bring the system or the network to a halt within seconds [11].

On the second of November, 1988 at the U.S. Cornell University Department of Computer Science graduate student, 23-year-old Morris wrote a worm and inserted it into the University computer network, resulting in the blockage of the network which has tens of thousands of computers. This accident is like a big earthquake in the computer industry, as this shocked the whole world and raised the fear of computer viruses. In the meanwhile, more attention and commitment are paid to anti-virus research by computer experts [11].

Viruses carry functions that are intelligent for providing protection in such a manner that detection becomes difficult for virus scanner. Viruses have to take various measures of intellect for survival. That is why they may have complex encrypting and decrypting engines. Encryption and decryption methods are used frequently by virus codes in current scenario .Viruses make use of these techniques to disguise the antivirus and to adopt the certain environment for their expansion [9]. Virus creators want to increment the lifetime of their produced viruses, so they constantly try to make the detection more difficult for antimalware designers and researchers working in this field [9].

Classification of computer viruses

Viruses are not found as standalone programs because they need host files for propagation. Based on evolution criteria computer viruses can be divided into following categories [9].

Encrypted virus

Encryption is the easiest approach adopted by virus code to avoid detection. The required purpose of encrypt or virus is to make change in their virus code with

the help of technique called encryption. This activity makes the virus body safe from the easy scan and thus provides safety to it. Encrypted virus generally contains two elements in it, the encrypted virus code, and a small decryption engine. CASCADE was the first virus of this category came into existence in 1988. [9].

Oligomorphic virus

Oligomorphic viruses change the decryptor body in the successive generation. To implement this technique the simplest way is to use large number of decryptors. Signature based detection requires the identification of predefined sequences that is not exact in this scenario. Signature based scanning is not at all fit to detect these type of viruses due to their adopted technique. The whole was the first virus that used this technique [9].

Polymorphic virus

Polymorphic virus attempts to hide the decrypting module. More complex methods are developed by virus designers to modify the code of virus file [8]. A third part to virus architecture has been added to Polymorphic malware. This part is mutation engine, it works against antivirus software attempts to find decryption routine. In the design of polymorphic virus, both the body of the virus and the mutation engine are encrypted. Mutation engine randomly generate new decryption routine, which has the ability to decrypt the virus and provides a very little similarities to previously generated decryption routines. So the virus body is encrypted and there is a different decryption routine for each infection. Based on this feature, a antivirus software that depends on finding decryption routine will fail to detect polymorphic virus. 1260 virus is an example of polymorphic virus which is written by wash burn in 1990 [9].

Metamorphic virus

The structures of the programs of metamorphic viruses are different in structure but it has the same malicious intent. The structure of metamorphic virus does include a constant virus body or the decryption routine. These types of viruses rewrite itself for each infection so at each infection attempt the virus is look completely as a new one. It has the ability to edit, retranslate and rewrite its code, so completely transform its shape. The techniques of code transformation is used to produce variants like code expansion, code permutation, code shrinking, garbage code insertion and register renaming. Metamorphic virus is classified as an epidemic virus which infects computers quickly and intensively. To have an efficient cyber defence against metamorphic malware, the classification of metamorphic malware must be defined and illustrated [7]. Metamorphic virus has the ability to mutate without changing its functionalities. Metamorphic virus represents a very dangerous threat, where a single virus file can appear as thousands of variants virus with totally different signature. Metamorphic viruses mutate their code in a specific manner very frequently and need to be prevented [12]. Metamorphic viruses do not use the techniques of encryption and decryption to hide their presence from antivirus engine. The main target of metamorphic viruses is to modify the signature while keeping the behaviour same. [9] Metamorphic virus modifies decrypt or as well as transforms their body at each generation. Latest virus generations has different forms they do not decrypt to a constant body of virus. Metamorphic virus appears different in successive generation [13]. This is illustrated in Figure-2.

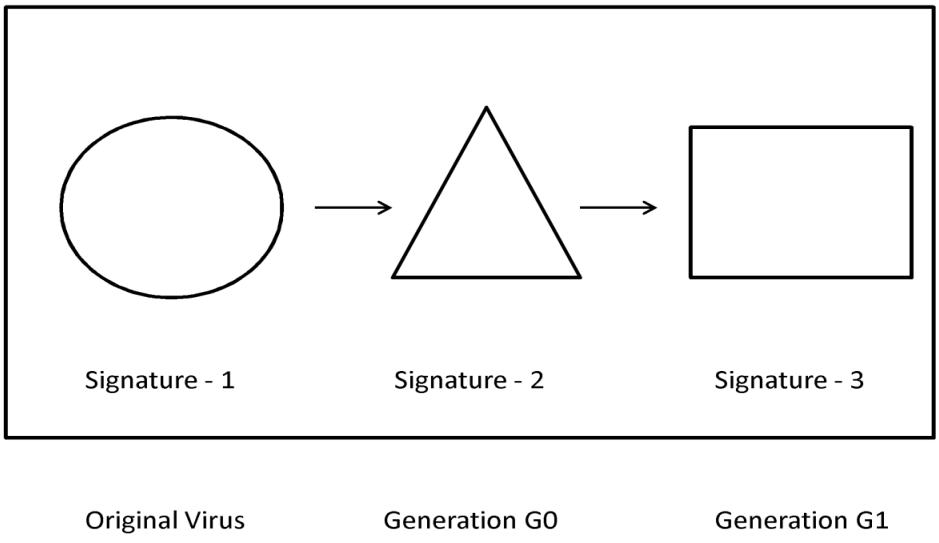

Figure-2. Metamorphic virus.

Worms

A computer worm is a standalone malicious computer program that can propagates itself across a network by exploiting security vulnerabilities or policy faults in widely spread services [14]. Worms and viruses are often having same behaviour or attack strategy; a worm has a very similar design to a virus. Different categorization considers worms as a sub-class of viruses. On the other hands, worms can exists as a standalone entity, worms doesn't attach itself to other files or application, it contains all the code that allow it to carry out its purposes and to survive itself from detection

History of worms

Worms has been considered as critical security threat in the internet since the late of 1980s. Worm's attacks have caused different damages. These damages include denying access temporary to different internet services, social disturbance and huge financial loss. One other the most lethal attack was the Code Red worm [15] which launched in 2001. This worm has infected about 359,000 devices within 24 hours only causing a horrible damage to their devices and networks. The Blaster worm [16] is another worm which discovered in 2003, this worm was targeting Microsoft windows and infected about 100,000 devices. This worm cost about US$299,579 as researches cost in nineteen universities to discover mechanisms to recover from this worm damages. Conficker worm was the most common worm attack. It has the fifth ranking global malicious threat which is reported Symantec in 2009. This worm infected about 6.5 million devices. The main idea of this worm is attacking Microsoft system vulnerabilities which related to update failure. Stuxnet worm, which is firstly discovered in June 2010, was one of the most sophisticated computer worm that ever discovered. In the first step of its propagation it target was Siemens industrial software and equipment. So this worm has used as a weapon in the information warfare worldwide to gather information and halt specific systems.

Worm attacks have about 25% of the total threats which is discovered in 2009 and nearly 20% of the overall threats in 2010. Detailed description of worms propagation mechanisms provides better understands of how it works and propagates. This can help to prevent worms from propagating and to mitigate the impact of worm's attacks. Moreover, it is very useful to have a full knowledge about the strength and weakness of current worm' propagation models, this can result in a potentially strong impact on predicting the spreading tendency of worms and developing an efficient defensive and preventive mechanism to mitigate worm's damages [17].

Worm categorization

A worm initialize it attack against a victim by scanning for vulnerabilities of the victim device. Worm can utilize different mechanisms to scan and discover new vulnerable device to compromise. Based on these vulnerabilities exploiting mechanism, worms can be categorized into two main taxonomies: topology based worms and scan based worms.

1. **Scan based worms:** in this type of worms , the worm scan the whole IPv4 address space or a subset of it, then it automatically, without any user interactions, start exploiting machine vulnerabilities and propagate to these devices. Different worms examples follow these mechanism, Code Red I v2 (2001) and Code Red II (2001) are examples of these worms. A scan based worms has a key characteristic, it can propagate through any topology without any dependency on the topology structure, which means that a compromised host can infect any arbitrary vulnerable host in that topology. Various scanning strategies, such as random scanning and localized scanning, can be employed to discover victims when they have no knowledge about vulnerable devices in the network. Worms using random scanning selects target IP addresses is a random fashion. On the other hand, localized scanning worms give a higher priority for close IP address rather than remote addresses when it start scanning for vulnerable devices.

2. **Topology based worms:** worms that depend on topologies to propagate like social media worms and emails worms. This type of worms depends on information retrieved from a compromised attack to make a list for targets to attack. By following this intelligent mechanism, worms can propagates more efficient than scan based worms which depend on making a large number of guesses to achieve successful infection. Topology based worms can spread in fast way since its target are in most of the times are successfully infected. Recent topology worms use social engineering techniques, this new techniques can prevent worm detection by most of the internet users, so finally they fail to detect malicious code and their machines become infected, this result in a wide range and fast speed of propagation. Spreading via topological neighbours is considering the key characteristic of a topology based. For email topology based worms, when a user browse a malicious email attachment ,the worm infect its system immediately and then it forward multiple worm email copies to compromised receiver email contacts list. Social network topology based worms like Koobface; the compromised account will automatically propagate malicious link or pages to all friends list and followed pages.

Worms propagation

A widespread concern and attention has been attracted to worms because of its ability to propagate from device to device and from a network to other networks. To limit the ability of worm widely propagation, vulnerabilities in the network must be explored and specified by deploying different worm discovery mechanisms. During the propagation of worms, devices can be found in one of three main states: susceptible, infected and cleared. A susceptible device is a device that has vulnerabilities and is a candidate to infection; infected devices are devices that has been compromised by the worm and can infect nearby devices; a cleared device is immune device which has no vulnerabilities and it has been infected and worms has been removed. Based on the probability of the infected devices to become susceptible again after recovery from worm attack, researchers have model worms propagation based on three major models. These models are: SI models, where infected devices can't be recovered, SIS models where infected devices can become susceptible again after recovery and finally SIR models where infected devices can be recovered. Based on these models, researchers proposed a different defence mechanism that works against worm's propagation. Despite the massive research efforts that have been proposed to stop worm's propagation, the attacks of worms still presenting a critical security threat to networks for multiple reasons. The first reason, worms can spread through the network in rapid way. This can be established by multiple means like email, files downloads, exploiting software security vulnerabilities, etc. worms can install itself on all vulnerable devices within few seconds[18]. The second reason is widespread and fast advances in the field of computer and network technologies which allow latest worms advances to be faster than prevention methods. The third reason is the increased complexity and efficiency of latest worms to be able to spread properly. Based on these reasons, it is very critical to describe the full details worm attack behaviours and investigate propagation mechanisms, which can provide efficient patch strategies for preventing worm's attacks on networks.

Target discovery techniques of worms

In this subsection, we discuss employ distinct propagation strategies such as random, localized, selective and topological scanning to spread, and some of their different sub-classes.

A. Scan based techniques

One of the most popular methods for propagation is scanning. Because of its implementation simplicity, it is the most widely employed method which is used by some well-known scan based worms [14].

1. **Random scanning:** in this approach, worms select candidate IP addresses randomly; this selection is leads to a fully connected topology with the same probability of infection β for each edge as illustrated in Figure-3. Different scanning strategies has been implemented based on ransom scanning, these strategies include hit-list, uniform, and routable scanning.

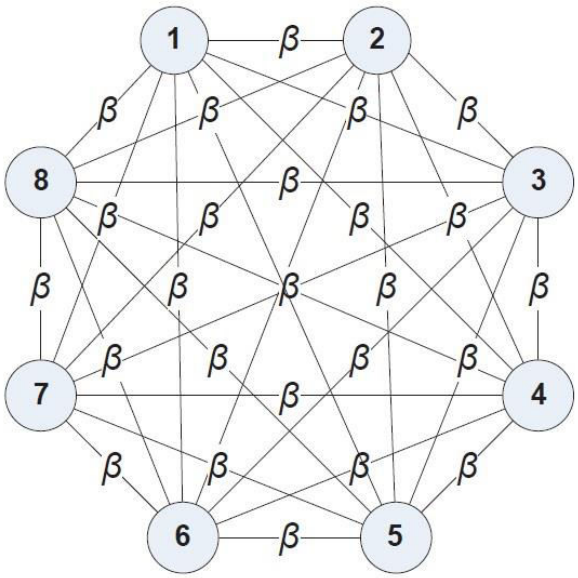

Figure-3. Graphical representation of random scanning.

a. **Uniform scanning:** this method follows the simplest way to select the targets. When there is now knowledge about the place of vulnerable devices, it selects devices addresses to probe from the whole IPv4 address space with the same probability. There is no reference for the selection process. a perfect random number generator is needed to generate list of IP addresses at random. An example of such common worms are Code Red I v1 and v2 [15].

b. **Hit list scanning:** this method was firstly proposed by Staniford *et al.* [18], by applying this method; infection time can be reduced efficiently at the early stage of the propagation of the worm. A hit list scanning worm start with scanning and infecting all vulnerable devices which can locate on the hit list, then it complete propagation using random method.

c. **Routable scanning:** This method scans on the routable address space instead of whole address space. So it is critical to specify which IP addresses are routable one

2. **Localized scanning:** in this approach of scanning, worms infect the nearby IP address instead of selecting

targets randomly. Localized scanning strategies scan devices in the local address space. Scanning nearby devices leads to a fully connected topology as illustrated in Figure-4, where devices within the same a single group either group1 or group 2, will infect each other with the same infection probability β1. On the other hand devices from different groups will infect each other with β2 infection probability.

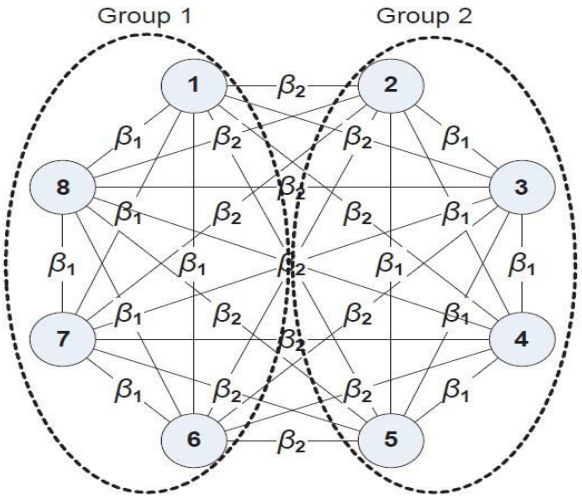

Figure-4. Graphical representation of localized scanning.

a. **Local preference scanning:** vulnerable devices are not uniformly distributed in the real networks. So scanning high density IP areas with high intense can result in fast and wide worm propagation.

b. **Local preference sequential scanning:** The sequential scanning approach, worms order the scanning process based on IP addresses in sequential order and begin with the starting IP address [19].

c. **Selective scanning:** this type of scanning is used when attackers plan to destroy a certain IP address range instead of the entire network address space. In this approach the probing space is reduced from the whole address space to those specified IP addresses range, it also results in an arbitrary topology as illustrated in figure 5. Device 4 scans devices 1, 8 and 7 with an infection probability of β. In target only scans approach, worm only scans and infects vulnerable devices in a specific target domain where selective scanning, attackers have higher concerns about the speed of propagation in the target domain than the infected network scale. Based on the investigation provided in [19], target only scanning can provide faster propagation if vulnerable devices are distributed in more density in the target domain or address space.

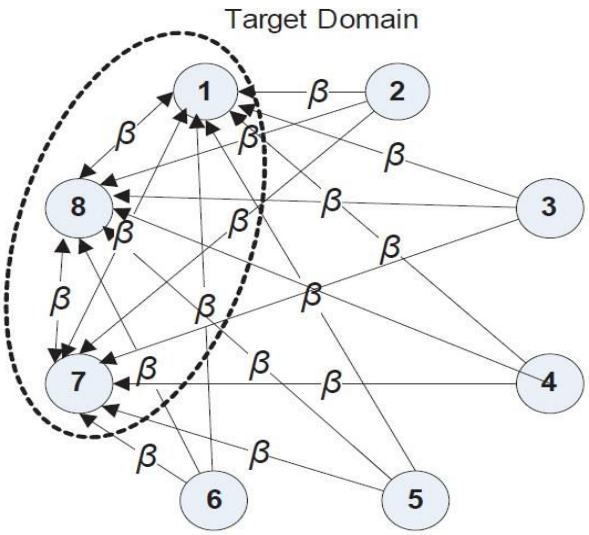

Figure-5. Graphical representation of selective scanning.

B. Topology-based techniques

Topological scanning techniques are fundamentally implemented by worms which use topological neighbours to propagate. Following this approach can result in an arbitrary topology, as illustrated in Figure 6, where device N_i , where i = 1, 2... 8, probes its neighbours with a various probability of infection β_i , where i = 1, 2... 10. Scanning topology described in this section reverberate the logical connection between the Internet users and social friend of the internet users. Email worms are examples of worms which implement a topology based techniques to initialize attacks. As a user receive an infected email in his mailbox and download or open the attached infected files, the worm code will infect the user device and start sending multiple copies to all of his mailing contacts found in the mail contact list. The recipient's machine addresses expose the relationship of neighbourhood. An example of email topology worm is Melissa [20] which launched in 1999; this worm sends a copy of itself to the first fifty email address that retrieved from all Outlook address books as it is activated by the first time when the infected file is opened. After Melissa, this type of email worms have become more disturbing popular, completed with toolkits. It has been improved by using social engineering mechanisms. An example for such worms is Love letter in 2000, My doom in 2004 and W32.Imsolk in 2010. Isomorphic worms have recently deployed topology based approaches. Examples for these worms include Bluetooth worms [21], p2p worms [22], [23], and social networks worms [24]. Koobface [25] propagation primarily depends on social networking websites and accounts. It traverses account friend list and then it post a links to videos that contains a copy of itself

on account friend's wall. As the user is tricked into visiting that posted video link, a prompt message to download an update for specific application or even a video codec is appeared. This message is actually a copy of that worm. It is not an easy mission to differentiate between a safe link posted by a friend and a link posted by a worm. Information retrieved from victim device can be utilized by topology based approach to find new targets and attack them. Using these smart mechanisms give these types of worm the power to propagate more efficiently than traditional scan based worms which depends on a large number of tries to achieve successful device infection. Instead, every attempt done by topology based worms are a successful infection step, so this worm propagates in a rapid manner.

Topology based approaches has common characteristic, user interference is needed to complete worm propagation. For example user need to download email attachment and open it to allow this worm to infect his device and propagates to his mail list addresses. So the ability to infect a device is depends and determined by human factors. These factors include the personal habits of user in checking emails and the user's security backgrounds and awareness.

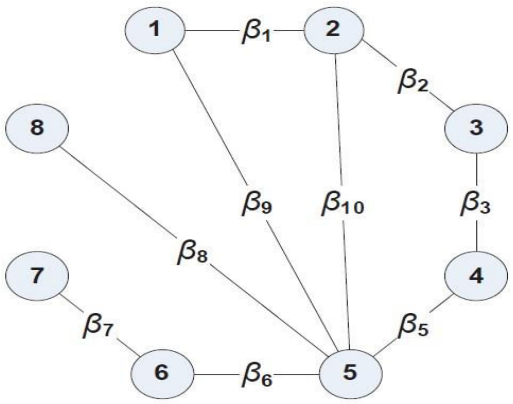

Figure-6. Graphical representation of topological scanning.

Topologies for modelling the propagation of worms

Network topology is considered as one of the most critical role in determining the efficiency of worm propagation. In this section, four typical topologies of networks has been introduced, these topologies are very common which used in worms propagation modelling.

A. Homogenous networks

Homogenous network characterized by equivalent device degree. The standard hyper cubic lattice and the fully connected topology are two typical homogeneous networks examples. The homogenous assumption is satisfied for the worm's propagation on homogenous networks where any infected device has an equal opportunity or probability to compromise any network vulnerable device.

B. Random networks

This kind of networks is a theoretical construct where links between nodes are selected randomly with equal probability, and example of such networks is ER (Erd¨os-Renyi) random network. This network use a random number generator, links are assigned from one node to another. Links which choose by random represent remote nodes shortcuts, so minimizing the length of path to otherwise distant hosts. A random network is considered as a non-homogenous network. This network node doesn't have the same degree. Random graph topology has a great impact on worm propagation speed and efficiency.

C. Small-world networks

This type of networks depends on mathematical graph. Mathematical graph inset between a random and a regular networks. It is implemented by replacing a fraction p of the links of a d dimensional lattice with new random links. Most nodes at small-world network are not neighbours, but on other hand, nodes are can be reached from any other node by traversing a small number of steps or hops. Small-world networks have a small characteristic path and are highly clustered.

D. Power-law networks

Power-law networks are defined as networks with a frequency fd of the out-degree d is proportional to the out-degree to the power of a constant α: fd ∝ dα. Where α is a constant called the power-law exponent? In this type of networks, nodes with the maximum topology degree are rare and the minimum topology degrees are popular.

E. Perspective of real world topologies

Topology based worms propagation is affected based on properties of the topology; this impact can make propagation and maintenance faster or slower.

The working mechanisms of worm

The working mechanism of worm is shown in Figure-7. Network worms attack can be divided into four phases, including information gathering, scanning probe, attack penetration and self-propulsion. Information collection mainly completes information collection of local hosts and target node hosts. Scanning probe mainly completes the detection of specific target host services vulnerabilities. Attacks permeability uses the found service vulnerabilities to carry out attacks. Self-propulsion completes the infection of target nodes. Worm uses system vulnerabilities to spread and host detection is carried out firstly. Good probe scanning strategy can accelerate the

worm propagation; idealized scanning strategy enables worms to find the possible infected hosts on the Internet in the shortest time. According to the way of the worm's choice of target address space classification, scanning strategies include selective random scanning, order scanning, scanning based on the target list, partition scanning, scanning based on the routing, scanning based on DNS.

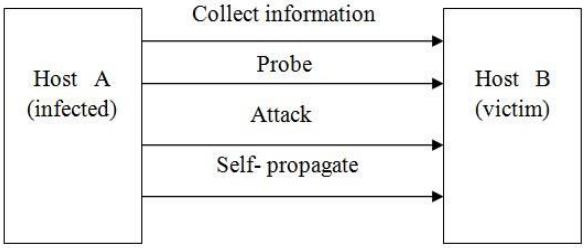

Figure-7. The working mechanism of worm.

The difference between virus and worms

The difference between traditional viruses, behavioural characteristics. Traditional worm and virus is contagious and has the characteristic of replication. It is very difficult to distinguish the two, especially in recent years, more and more traditional virus takes a part of the worm virus technology, on the other hand, destructive worm also took part of technology of the traditional virus. The difference between worm and traditional virus is shown in table 1. Study and research is carried out on foundation of traditional virus and relative content of emerging virus.

Table-1. The difference between worm and traditional virus.

	virus	worm
form	parasitic	individual
copy form	inserted into the host program	a copy of itself
transmission mechanism	a host program running	system loophole
target	local file	other computers on the network
trigger contagion	computer users	computer users
impact	file system	network performance, system performance
The role of the user	The key links in propagation	Irrelevant
prevention and control measures	removed from the host file	system patch
the main against body	anti-virus vendors	network managers

From the above comparison, it can be found that the traditional virus mainly attack file system. In the process of its transmission, computer users are catching trigger, which is a key link in the process of transmission, the user's level of computer knowledge often determines damage degree caused by the traditional virus. And worm

mainly uses computer system vulnerabilities to infect. In the process of transmission, it has nothing to do with whether to operate computer, which has nothing to do with the user's computer knowledge level.

Bots

Bots is considered as one of the most lethal attack in the internet. Hundreds of scientific research have been proposed on bots behaviour, detection and mitigating. In this report we will describe the concept of bots, how it works, how it spread and how we can detect and mitigate this type of attack [26]. A bots is a group of hacked machines which is called bots; these bots are controlled by a single or a group of control servers which are directed by the botmaster. Botmaster is the human who control the whole attack, issuing command, receive data and direct the bots based on his purpose.

In most cases the botmaster doesn't command the control server directly, there is always a relay networks which consist of hacked devices works as proxies[27]. These proxies are called steeping-stones. Figure-8 shows the structure of bots attack and how the botmaster can control and communicate with bots to initialize an attack.

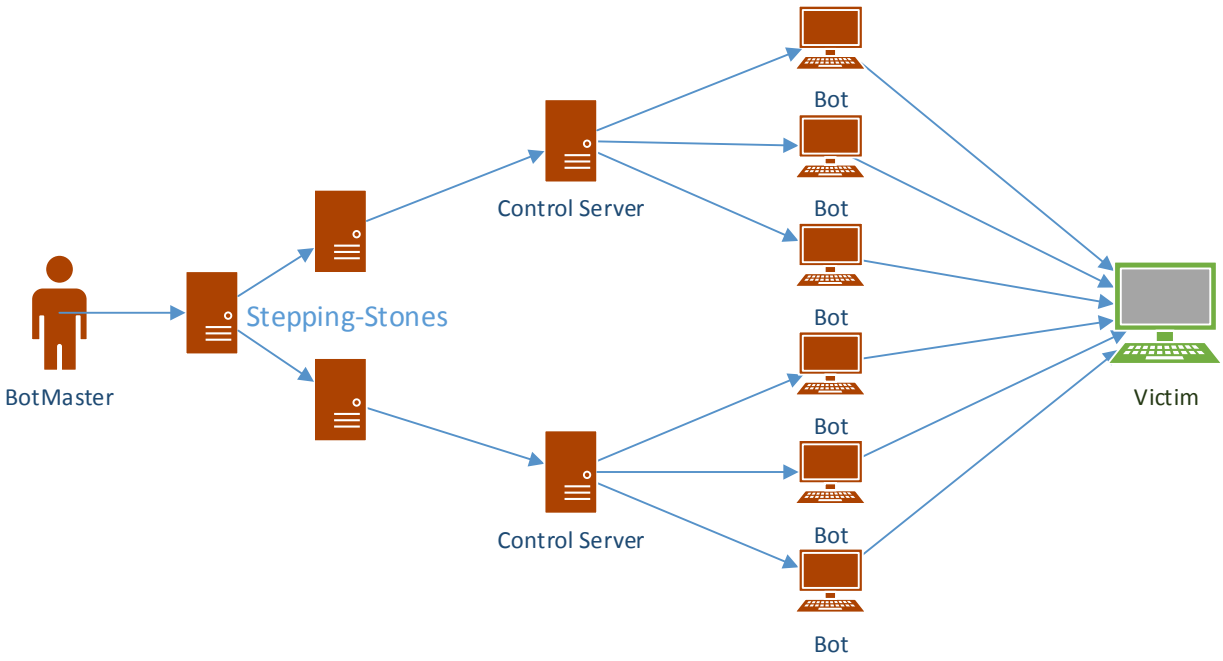

Figure-8. Bots structure.

The main goal for using bots is to perform different types of malicious activates. These activities can have different goals these goals can be categorized as follows:

1- **Traffic reconnaissance:** host traffic monitoring can be used to gather information. This information can be used to osculate the attack or it can be used to steal secret or financial information like user credentials or bank accounts.

2- **Denial of service attack:** bots can be used to start a distributed denial of service attack against specific organization or corporation. This type of attack can be used to stop the service that provided by that organization.

3- **High computing power:** combining the resources available at the bots can be results in a high computing poser which can be used to be used to crack a password or any high computational issue.

4- **Spam marketing:** Marketing using the internet is considered as one of the most effective way to announce products since it cheap and easy. Botmaster can use bots to send SPAM emails which is very difficult to be discovered.

5- **Malware distribution:** bots can be used to spread malware on the networks where bots located. This malware can be used to infect more machines and initialize further attacks [28].

How bots work?

The life cycle of the bots can be divided into four stages: infection, spreading, rallying and elusion. In this section we will describe each stage.

1- Infection: a host is infected when the bots binary is successfully run on that host.

2- Spreading: the main goal of the bots is continuously spreading the bot binary across vulnerable devices and increases the number of bots. Spreading mechanisms can be categorized into two types: active and passive [29]. In active spreading the bots can locate and infected other vulnerable hosts automatically without any user interaction. In this type the bots scan his nearby machines for vulnerabilities and exploit these vulnerabilities to invade these hosts. On the other hands passive spreading require some user interaction. Different mechanism can be used in passive spreading includes : downloading bots binary from a hacked or fake websites , transferring bots binary from an infected media or shared folder and get bots binary using social networks by infected pages and accounts.

3- Rallying: bots without the control servers is just an infected device that doesn't have any purpose[30]. When the bots binary executed it start looking for his control server to communicate with. Bots can use control server IP address or domain name to reach it. IP address or domain name can be included in the bots binary or can be generated by an algorithm used by bots.

4- Elusion: bots have to survive for the longest time, to achieve this it use different mechanism to hide its activities and communication with the control server.

a. To hide the bots activates bots change its binary and shapes to mitigate any pattern based detection mechanism by using polymorphism which allows bots binary to appear in different shapes. Disable any security application on infected machine is another mechanism to avoid bots discover where using root kit approach can be more effective which can bypass the whole operating system[31].

b. Communication elusion with control server can be more critical since it easier to discover. Different approaches can be used to hide the communication with the control server: bots use IP Flux to change the domain name IP address frequently. Bots can also use domain Flux which can be used to frequently change the domain name using wildcarding. Another elusion mechanism can be implemented using a rogue DNS server which can be installed on one of the bots that has been hacked. Bots also can use anonym zed networks which prevent the ability to trace back the source of the connection. Encryption and tunneling are used approaches which help bots to hide the details of the connection between bots and control servers [32]. Figure-9 show the life cycle of the bots.

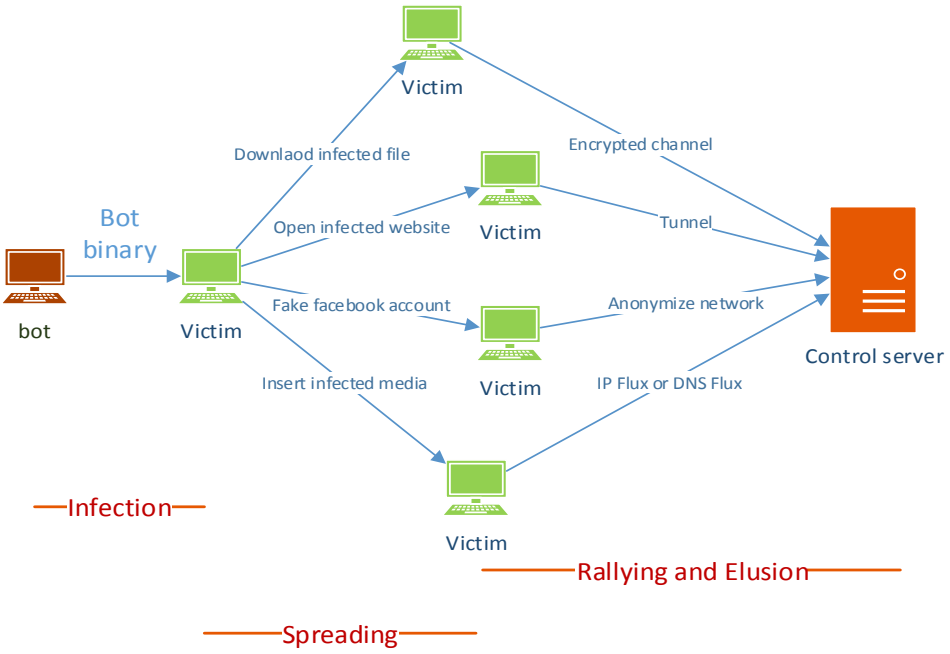

Figure-9. Bots life cycle.

How to detect bots?

The detection of the bots can be achieved using one of three ways: bots detection, control server detection

and bots master detection. Detection of botmaster can lead to collapse the whole members of the bots structure both bots and control server where control server detection expose only the bots. Different mechanism can be used to detect each member of bots structure. Each member detection can be categorized into two types active and passive. In active approach the detector agent incarnate as a part of the bots to figure out how it works and discover related bots and control server where passive detecting related to just monitoring and analyzing of bots activities.

Bots detection

For active bots detection there is two mechanism infiltration and control server hijack. In infiltration a detector machine is work exactly as a bots. This allows the detector to discover the control server and other bots and take them down. For the second methods detector can use information sniffed from the rallying stage to hijack control server [33]. This can lead to discover all bots controlled by this server.

In passive detection detector can silently monitor and analyse the traffic of bots without any interfering or traffic manipulating. And this type of detection has two types syntactic and semantic. For syntactic approach detector identify the bots by comparing its behaviour with a pre-defined patterns of bots behaviour, these patterns are extracted from previous samples. Semantic approach use the protocol information and event context to detect bots infection this can be accomplished suing similarity and behavioural analysis [34].

Control server detection

Detection of control server can expose all bots that communicating with the exposed server. Active server detection method performs a part of bots communication. This active detection can be categorized into two methods injection and suppression. For injection method it inject manipulated packets into suspected network flow and determine who respond to such packets where suppressed method rely on suppressing on suspected network traffic packets to retrieve response and recognize the control server.

Passive control server detection rely on monitoring and analysing its activity without any interference or interaction and it is like bots detection can be implemented using two ways syntactic and semantic [35]. In syntactic a developed signature based models are used to compare recent traffic with predefine malicious traffic patterns where semantic detection rely on heuristic to make a link between current traffic and the behaviour of control server traffic, different ways can be used to find similarity these ways includes statistical approach, correlation and behaviour based methods.

Botmaster detection

Botmaster detection is very complicated and detecting botmaster can have a catastrophic effects on bots structure it could impose all its member including bots and control server. Botmaster has the highest security protection [36]. Active botmaster detection depends on simulating bots traffic with high technique; the most common technique is marking which is used to trace back hacking traffic. In passive botmaster detection two main approach have been used stepping stone detection and logging,

Botmaster always hides behind a stepping stone so detecting stepping stone can lead to detect botmaster. Detecting steppingstone rely on correlation of traffic content, machine activity and timing. For logging routers log and analyse each packet and specify if these packets are forwarded from predefined routers. This approach required high computational capabilities.

How to defence bots?

Avoiding bots infection and mitigate bots attack can safe all of the detection efforts. Botnet defence can be in one of two approaches: remedial approach or preventive approach.

- **Preventive approach**

In this approach hosts has to perform proactive steps to avoid any bots attacks. This approach can be implemented in different direction, the first direction is the technical direction which include host cleanliness by guaranteeing latest security patches using auto update system and implementing security best practice steps [37]. These steps can include installing host intrusion prevention application. Technical direction can also include network cleanliness by implementing network anomaly detection system which can discover any malicious activities in the network. The second directions are the non-technical direction which is not related to any technical procedure. This direction focus on user's awareness. This direction can be implemented by different steps like attackers deterrence by applying more sanctions and financial penalties on attackers, legal framework for defence mechanism against bots can be a great step for prevent this type of attacks. Finally user education can play a critical role in preventing any vulnerability which can be exploited by bots

- **Remedial approach**

This type of defence can help to recover from bots attack partially or completely. This approach is working on two directions removing the bots which called defensive direction or destroying the bots structure which is called offensive direction.

- **Defensive mechanism**

These mechanisms work on recovery from bots infection and it has two main categories host based and network based. Host based mechanism works on restore the clean state of an infected bots either by disinfecting the bots using dedicated application or by reinstallation of a new operating system to confirm that bots binary completely cleared. Network based mechanism works on cleaning and securing the network infrastructure. Blocking bots by quarantining infected machine and blocking any control server communication can make the network clean and stop bots binary activity and spreading.

- **Offensive mechanism**

This mechanisms work on launch a direct or indirect attack against bots to destroy the bots infrastructure, indirect attack goal is to minimize the bots usability by injecting fake information like fake credentials or band accounts [38, 39]. Direct attacks works on destroying the members of bots structure. Targeting bots binary which always has too much bugs can affected its functionality. Injecting poisoned command for control serves can disturb bots communication.

Table-2. Summary of latest related research.

Author	Titles	Method	Description
Wang, Y., Wen, S., Xiang, Y., & Zhou, W.**(2014)**	Modeling the Propagation of Worms in Networks: A Survey	This paper presents a survey and comparison of worms' propagation models according to two different spreading methods of worms. First identify worms characteristics through their spreading behavior, and then classify various target discover techniques employed by them.	There are the two common means for propagating worms: scanning vulnerable computers in the network and spreading through topological neighbors. Modeling the propagation of worms can help us understand how worms spread and devise effective defense strategies. However, most previous researches either focus on their proposed work or pay attention to exploring detection and defense system. Few of them gives a comprehensive analysis in modeling the propagation of worms which is helpful for developing defense mechanism against worms' spreading.
Guohua, Z. **(2015)**	Anti-Virus System Structure Analysis and Design under Network Environment	Designed the enterprise network security scheme, this system can provide information security management with a more comprehensive, convenient, intuitive, accurate virus monitoring platform, reduce damage and risk caused by growing virus on network, and provide security for the enterprise's informatization Construction.	The current network security technologies are reviewed, the present situation and the demand of network security is analyzed; the key network security technology is investigated. Starting from the enterprise information safety, the network virus, access control and information system Stability is analyzed. On this basis, the enterprise network security scheme is designed.

Khattak, S., Ramay, N. R., Khan, K. R., Syed, A., & Khayam, S. A. **(2014)**	A Taxonomy of Botnet Behavior, Detection, and Defense	In this paper, bots literature has been described into three main taxonomies. These taxonomies are bots life cycle and goals, detection approaches and finally defense approaches. These information are provided to allow researchers to investigate and propose novel methods for detection and protections.	Bots has the highest portion of internet attacks. Bots spread by bots binary which infect vulnerable devices which become bots, these bots communicate with control server to get directions which issued by botmaster. Bots attacks have many malicious purposes to steal information and cause damages. To survive for the longest time, bots has many elusion techniques to hide itself and its communications. To detect bots, different techniques have been provided to detect bots binary, bots communication with control server and finally detecting botmaster which can lead to discover all bots structure.
Bist, A.S. **(2014)**	Detection of Metamorphic Viruses: A Survey	presented a identification techniques used for metamorphic viruses	Computer viruses are big problem for security. It is essential to differentiate between reproducing programs and its Similar forms. Reproducing programs will not necessarily harm the system. Classification aspect of metamorphic viruses is an emerging issue of research.

3. CONCLUSIONS

This paper explains in detail about identification techniques used for viruses, worms and bots. Biological epidemiology study has been extended to provide better description of how and when computer viruses propagate. Developed techniques to help us to achieve the safety and effectiveness of anti-virus technology have been described. These developed technologies are able to deal with known viruses with an efficient and successful way, and it is also being developed to extend its ability to automatically work with previously unknown viruses.

Worms and their variants behaviour has been described as one of the most critical challenges for network security researchers. Worm's propagation mechanism has been investigated and description about how it has evolved with the proliferation of data transmission, instant messages and other communication technologies has been described. The main two worm propagation topologies, scan-based techniques and topology-based techniques are described and investigated. Where understanding worm propagation models can help us to efficiently understand how worms propagate and allow researchers to propose defence strategies with high efficiency. Different models have been proposed for modelling the mechanism of propagation. Measuring Worms categories: worm virus can automatically spread

through the internet. If there is any vulnerability, the computer will be infected. Even though antivirus software can kill the virus, the computer resource will be consumed. If there is any computer without valid antivirus software, worm virus will detect all the computers in this network. In the last five years, the number of internet connected users has been doubled. Advances in the field of wireless networks and communication are expected to increase the rate of the internet connected users many times. However, the security awareness of these increased users is disproportionate to the growth of their numbers. The next level of network attack represented by bots can be very harmful and cause wide and very fast internet resources damages. Different mechanisms can be used to compromise users' devices. A bots has different strategy to attack devices, botmaster can control bots via control and communication server where he can oscillate it attack and make it more harmful. This survey firstly introduced the target discovery techniques for viruses, worms and bots. Secondly, it analysed the types and characteristics of viruses, worms and bots. Finally, this survey has described some typical mathematical models of viruses, worms and bots.

REFERENCES

[1] Liu J.-W. 2009. Research of Intranet Network Security Architecture Base on Firewall and VPN. Science Technology and Engineering 04.

[2] Liu D.-P., Dong X.-H., Zhang M.-W., Chen J. 2009. Cloud method of multi-granularity network security situation analysis. Journal of Computer Applications 02.

[3] Wu Peng. 2012. Analysis and Exploration of Related Issues on the Computer Network Security Based on Firewall and Anti-Virus Software, Advanced Technology in Teaching-Proceedings of the 2009 3rd International Conference on Teaching and Computational Science (WTCS 2009) Advances in Intelligent and Soft Computing. 117: 45-49.

[4] Rajab M.A., Ballard L., Mavrommatis P., Provos N., Zhao X. 2010. The Nocebo Effect on the Web: An Analysis of Fake Anti-Virus Distribution. In: Workshop on Large-Scale Exploits and Emergent Threats.

[5] Stone-Gross B., Abman R., Kemmerer R., Kruegel C., Steigerwald D., Vigna G. 2011. The Underground Economy of Fake Antivirus Software. In: Proceedings of the Workshop on Economics of Information Security, WEIS.

[6] Fossi M., Turner D., Johnson E., Mack T., Adams T., Blackbird J., Low M.K., McKinney D., Dacier M., Keromytis A., Leita C., Cova M., Overton J., Thonnard O. 2009. Symantec report on rogue security software. Technical report, Symantec.

[7] Prasad T.S. and N.R. Kisore. 2015. Application of Hidden Markov Model for classifying metamorphic virus. In: Advance Computing Conference (IACC), 2015 IEEE International. IEEE.

[8] Aycock J. 2006. Computer viruses and malware. Vol. 22. Springer Science and Business Media.

[9] Bist A.S. 2014. Detection of metamorphic viruses: A survey. In: Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. IEEE.

[10] Miao, Q., *et al.* 2015. Malware detection using bilayer behavior abstraction and improved one-class support vector machines. International Journal of Information Security. p. 1-19.

[11] Elloumi M., *et al.* 2013. Comparison for the detection of virus and spam using pattern matching tools. in Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), 2013 International Conference on. IEEE.

[12] Bidgoli H. 2006. Handbook of Information Security, Information Warfare, Social, Legal, and International Issues and Security Foundations. Vol. 2. John Wiley and Sons.

[13] Jordan M. 2002. Dealing with metamorphism. Virus Bulletin. 1(10): 4-6.

[14] N. Weaver, V. Paxson, S. Staniford and R. Cunningham. 2003. A taxonomy of computer worms. in Proc. 2003 ACM workshop on Rapid malcode. ACM, pp. 11-18. [Online]. Available: http://dl.acm.org/citation.cfm?id=948190.

[15] D. Moore, C. Shannon et al. 2002. Code-red: a case study on the spread and victims of an internet worm. In: Proc. 2nd ACM SIGCOMM Workshop on Internet measurement. ACM, pp. 273-284. [Online]. Available: http://dl.acm.org/citation.cfm?id=637244.

[16] H. V. Poor. 1988. An introduction to signal detection and estimation. New York, Springer-Verlag. 1: 559.

[17] J. Hu, X. Yu, D. Qiu, and H.-H. Chen, "A simple and efficient hidden markov model scheme for host-based anomaly intrusion detection. IEEE Network. 23(1): 42-47, 2009. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs all.jsp?arnumber=4804323.

[18] S. Staniford, V. Paxson, N. Weaver et al. 2002. How to own the internet in your spare time. In: USENIX Security Symp. pp. 149-167.

[19] C. C. Zou, D. Towsley and W. Gong. 2006. On the performance of internet worm scanning strategies. Performance Evaluation. 63(7): 700-723, [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016 6531605001112.

[20] N. Weaver. 2001. A brief history of the worm. Security Focus Online. Vol. 261.

[21] G. Yan and S. Eidenbenz. 2009. Modeling propagation dynamics of bluetooth worms (extended version). IEEE Trans. Mobile Computing. 8(3): 353-368. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs all.jsp?arnumber=4624266.

[22] X. Fan and Y. Xiang. 2010. Modeling the propagation of peer-to-peer worms. Future generation computer systems. 26(8): 1433–1443. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016 7739X10000737.

[23] R. W. Thommes and M. Coates. 2006. Epidemiological modelling of peerto- peer viruses and pollution. in INFOCOM. 6: 1-12.

[24] W. Fan and K. Yeung. 2011. Online social networks paradise of computer viruses. Physica A: Statistical Mechanics and its Applications. 390(2): 189-197. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S037 8437110008344.

[25] W32.koobface. [Online]. Available: http://www.symantec.com/security response/writeup.jsp? docid =2008- 080315-0217-99.

[26] Cole, A., M. Mellor, and D. Noyes. Botnets: The rise of the machines. In: Proceedings on the 6th Annual Security Conference. 2007.

[27] Ollmann, G., Botnet communication topologies. Retrieved September, 2009. 30: p. 2009.

[28] Chen T. 2010. Stuxnet the real start of cyber warfare? [Editor's Note]. Network, IEEE. 24(6): 2-3.

[29] Khattak S., et al. 2014. Taxonomy of botnet behavior, detection, and defense. Communications Surveys and Tutorials, IEEE. 16(2): 898-924.

[30] Dagon D., *et al.* 2007. A taxonomy of botnet structures. in Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual. IEEE.

[31] Brown D. 2010. Resilient botnet command and control with tor. DEF CON. p.18.

[32] Barford, P. and V. Yegneswaran, An inside look at botnets, in Malware Detection. 2007, Springer. p. 171-191.

[33] Choi H., *et al.* 2007. Botnet detection by monitoring group activities in DNS traffic. In: Computer and Information Technology. CIT 2007. 7th IEEE International Conference on. IEEE.

[34] Strayer, W.T., *et al.* 2008. Botnet detection based on network behavior, in Botnet Detection. Springer. pp. 1-24.

[35] Karasaridis A., B. Rexroad and D. Hoeflin. 2007. Wide-scale botnet detection and characterization. In: Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets. Cambridge, MA.

[36] Feily M., A. Shahrestani and S. Ramadass. 2009. A survey of botnet and botnet detection. In: Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. Third International Conference on. IEEE.

[37] Kotenko I., A. Konovalov and A. Shorov. 2010. Agent-based modeling and simulation of botnets and botnet defense. In: Conference on Cyber Conflict. CCD COE Publications. Tallinn, Estonia.

[38] Bailey M., *et al.* 2009. A survey of botnet technology and defenses. In: Conference For Homeland Security, 2009. CATCH'09. Cybersecurity Applications and Technology. IEEE.

[39] Mostafa, S., Saad, H., Jaber, M. M., Ali, M. H., & Dhafer, K. (2016). The Design Trends of Keystream Generator for Stream Cipher for High Immunity Attacks. In Advanced Computer and Communication Engineering Technology (pp. 877-889). Springer International Publishing.