Comprehensive Study on Computer Worm – Cyber Attack

Valliammal.N
Assistant Professor (SS), Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamilnadu, India.

Abstract – Due to tremendous growth of Internet, the huge of data transaction is done through network in the communication fields. With these rapid developments of Internet applications, hackers or attackers spreads attacks that are also increasing. Worm attack is one of the major security threats among all attack that affect the data. This worms are significantly affected the Internet infrastructures through their various vulnerable exploitation in operating systems, programs and applications. In this paper, characteristics of worm, type of worms based on vulnerability and countermeasure approaches to defend the worms are discussed.

Index Terms – Cyber security, cyber-attack, malware, worm, containment approaches.

1. INTRODUCTION

Cyber Space is a common place for disgruntled employees and hackers to commit many cyber-attacks. The major goal of a cyber-attack is to damage the *function* of a computer network. The various ways are needed to compromise a computer network. Syntactic attacks affect the computer's operating system that leads to cause the network to malfunction. Examples of this attack are "worms, viruses, Trojan horses and denial of service attacks [1]. Semantic attacks keep the operating system as usual but compromise information accuracy it processes and to which it reacts. . Hence, computing system under semantic attack works and will be seemed as operating properly, but it will produce results at variance with reality. There are numerous hacking activities happening on the internet in which one of the dangerous threats is worm attack. These attacks cause lots of loss for business resources, financial damages and also they lead to cyber-attacks against countries [2]. Recovering from attacks is more cost than implementing a network. Currently, there has been a lot of attention around "an international ransomware attack". This ransomware called WannaCry that encrypts the computer's hard disk drive and then propagates between computers on the LAN[3]. This attack infects the computer using multiple methods such as within word documents, PDFs and other files usually sent through phishing emails and on unpatched systems as a computer worm.

2. GROWTH OF CYBER-ATTACK CASES IN INDIA

The statistics have been demonstrated that the seriousness of Cyber-attacks in India. The country has registered 107% of CAGR (Common Annual Growth Rate) in the number of Cyber-attacks registered in last few years. Figure 2.1 shows that growth of cyber-attacks in India on yearly basis. The survey shows that the number of attacks increases year by year rapidly [4].

Nearly 13,301 Cyber-attack cases were registered in 2011. The number is increased by almost 50 percent in the following year, reaching 22,601. The statistics of 2013 stupor people as it shows the unexpected increase, making the count of cyber-attacks cases reach 71,708. Surprisingly, in 2014 the number of cases registered under Cyber-attacks laws is increased by more than 100% to 1, 49,254.

The mobile frauds became major concern for various organizations as 35-40% of financial transactions are done through mobile devices and this infection rate is increased up to 55-60% by 2015.Cyber-attacks have become more frequent and costly to individual users, businesses, economies and other critical infrastructure components.

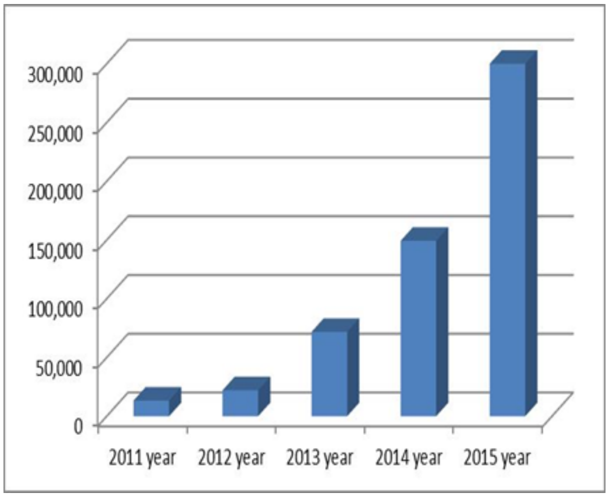

Figure 2.1 Growth of cyber-attacks in India

3. SECURITY THREAT

A security threat[5] to a system is a set of situations that has the potential to cause loss or harm. *"A threat is blocked by control of vulnerability."* The below figure 3.1 represents security threats classification.

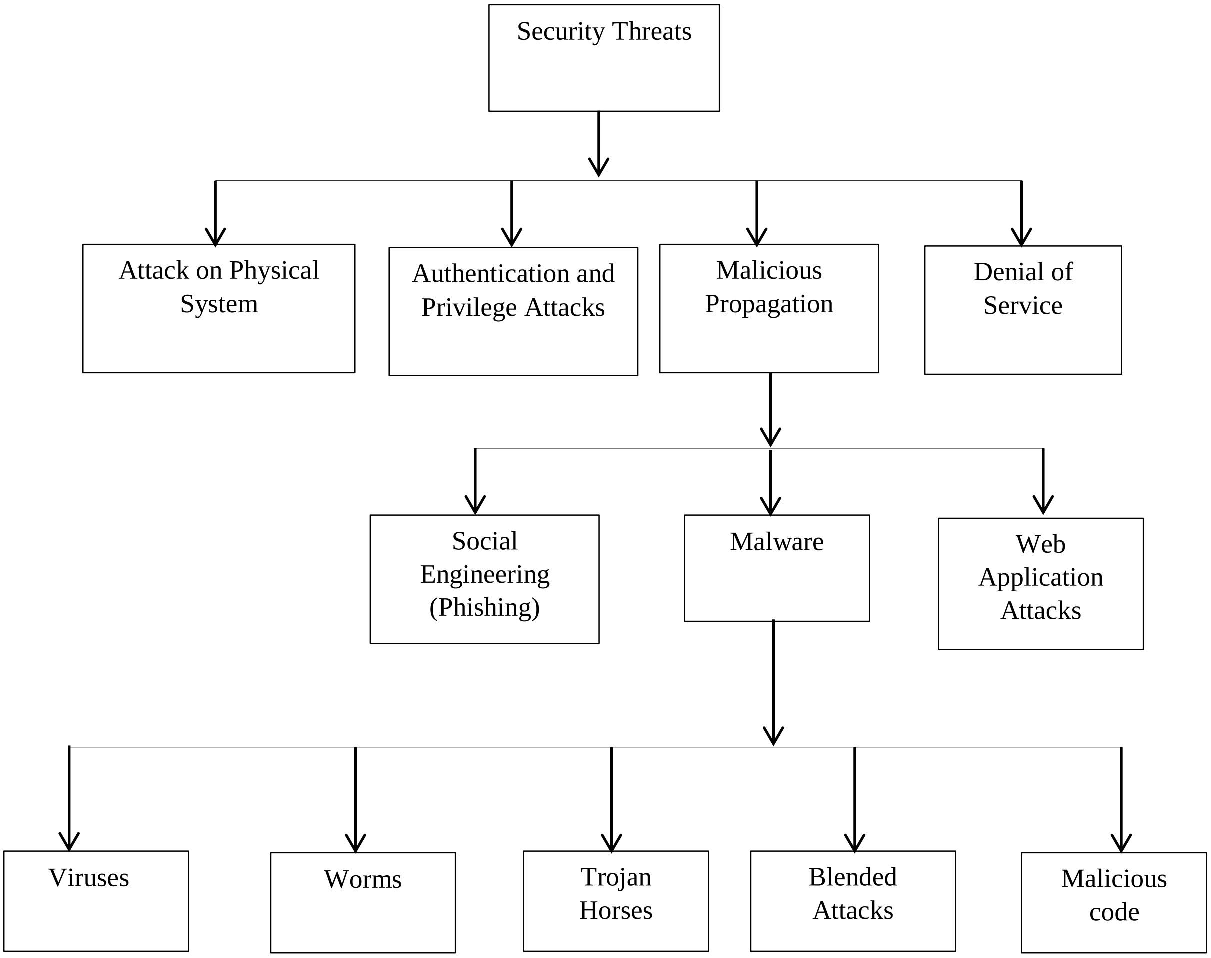

Figure 3.1 Classification of Security Threat

3.1 Authentication and privilege attack

In many systems, a password remains vulnerable. A system administrator has full access privileges and may leak out the sensitive information that significantly causes the stability and reputation of the company. No encryption is used in many cases that allow anyone can view and modify the network traffic easily.

3.2 Attack on physical system

The number of different methods allows attackers who can do unauthorized access to company wireless and wired networks. Accidental association is one of methods for this unauthorized access. If user logs into a computer and bolts on to a wireless access point through neighboring companies overlapping network, the user can't recognize that attack has occurred. Therefore, proprietary company information is unprotected and there may happen a link from one company to the other.

3.3 Denial of Service (DoS) Attack

This attack avoids users from making use of a resource in a computer or network and target the computer network connectivity or bandwidth. This attack is also called Bandwidth attacks that prevent the usage of the network with huge volume of traffic and all available network resources are consumed. Therefore, user requests cannot process in the network for these circumstances.

3.4 Malicious propagation

Tampering the computer system includes penetration, Trojan horse virus and the generation of illegal codes to alter the standard codes within the system. This type of operation can be termed as malicious misuse [6]. The various categories of malicious propagation are listed below:

- Social Engineering - Virus writers, Scare ware vendors and Phishers are users of Social Engineering.
- Attacks on web Applications - Attacks when users visit a website, clicking in an E-mail or link from Social Engineering site and visiting a legitimate website.
- Drive-by downloads attack - Causes threats such as log keystrokes, rootkit, herd system into botnet and infect web browser with Trojan Horse.

4. WORM

A worm is a self-propagating computer program, which is often designed to cause harm to a computer and/or a computer network[7]. A computer worm self-propagates by sending copies of itself from one node to another (e.g., from one computer to another) over a network. Such transmissions can occur without any user intervention, thereby allowing them to be spread quickly and easily. An attack that aims to spread a worm on the Internet has two main purposes:

- To cause a traffic overloading local area networks and congestion on Internet links, which disrupts affected hosts and leads to financial losses; and
- To recruit compromised hosts for future use.

4.1 Statistical report on worm attack

The Statistical report on worm attack is given below [8]

- In 1988, Morris worm caused $10 to $100 million in damage on the young Internet of 60,000 computers.
- The Code Red worm marked the dawn of modern worms. In July 2001, the worm infected 359,000 hosts world-wide within 14 hours. Code Red II utilized an effective localized scanning strategy and carried a payload that established a backdoor. This worm caused $2.5 billion financial loss.
- The multi-exploit worm Nimda passed through many firewalls and other defenses by using five separate mechanisms by which to spread and propagate.
- Slapper controlled infected machines by establishing a Peer-to-Peer (p2p) network.
- In 2002, the Slammer worm spread at impressive rates by infecting 90% of the vulnerable hosts within 10 minutes. Slammer, sometimes called Sapphire, spread at unbelievable rates by infecting 90% of the vulnerable hosts within 10 minutes, resulting in a population doubling time of 8.5 seconds. In 2003, This worm infected 75,000 Computers , damaged MS SQL servers and achieved 55 million scans in 3minutes
- In 2004, witty worm infected 12,000 hosts in 45 minutes
- The Leaves worm was arguably one of the first stealth worms. It infected machines stricken with the Sub Seven Trojan, assumed control of the machine and the Trojan, and pointed the computer to an IRC channel to await commands. Leaves showed the potential danger involved with the merger of self-propagating code and DDoS tools.
- In 2007, storm worm created infection to Tens of Millions of hosts. In 2008 , Conficker worm infected 90%of susceptible hosts within minutes and controlled 6.4 million hosts
- In 2011, Spy Eye and Zeus merged code and attacked on mobile phone banking information. Anti-Spyware 2011, attacked Windows 9x, 2000, XP, Vista, and Windows7.
- In 2012, Flame also known as Flamer, sky Wiper, and Sky wiper attacked computers running Microsoft Windows.
- In 2012, stuxnet worm created cyber war. In 2013, welchia exploit their impact on windows 2000,NT and windows XP . In 2014, Win32.IRCBot worm transferred confidential information to hacker
- On Friday, 12 May 2017, a large cyber-attack called WannaCry attack was launched, infecting over 230,000 computers in 150 countries, demanding ransom payments, reported by Wikipedia.

Recently, Kaspersky, a Russian anti-virus company reported that India was one of the countries poorly infected by the WannaCry attack. In India, this attack caused around five per cent of all computers affected in the attack. News agency IANS reported that this attack infected 18 units of police computers in Andhra Pradesh's Chittoor, Krishna, Guntur, etc.

4.2 Worm vulnerability

Worm uses multiple vulnerabilities to spread [9], such as

- Remote Procedure Calls -use remote execution of a program. After the worm propagates itself to any host, it sends DOS attack and provides backdoors to attackers. Then, this worm will find new hosts to infect with port 80 on TCP.
- Buffer Overflows - where in data is stored in memory location other than the memory allocated by the programmer. Buffer overflow vulnerability allows executable malevolent code to be copied into the memory of a target computer. A skillful attacker can then manipulate the invaded computer to remotely execute the injected code.
- Remote Command Execution - running a shell command remotely on a different host.
- Cross-site scripting vulnerabilities -allow the adversary to inject malicious links in the web interface. During execution of such a link, the malware is automatically downloaded into the server. The hackers can insert a code to perform drive-by download attacks or further spread the vulnerabilities of the active web server to rise growth of the infection rate.

4.4 Characteristics of worm attacks

The life of the worm is classified into finding the target, transferring the worms, activation of transferred worms and worm infection. The worm attacks characteristics are further categorized in depth as shown in

S.No	Worms	Characteristics
1.	P2P	- Hazard to Internet infrastructure.. - Live streaming applications. - P2P users for content distribution.
2.	E-mail	- Spams in mailboxes. - Advertisement bots on instant messaging communities - Publicity included in wikis - Unwanted SMS communications.
3.	IM	- Hazard to home IM users and organizations that allow IM in workplace. - Outbreak of zero-day IM malware, lack to protect enterprise-like networks..
4.	Internet	- Hazard to network security community.. - use P2P vulnerabilities to propagate themselves in the network

Table 4.1. Categories of Worm

4.4.1Target finding scheme

When the worm enters into the network, its initial step is finding targets to spread and exploit [11][12]. Blind target scanning, hit list scanning, topological scanning and web search are various finding target schemes of worm.

- Blind scan Internet worms don't offer earlier information about the targets and create number of failure connection rate.
- Hit list worms accomplish its attack using available pre-scanned vulnerable addresses. Hosts are associated with the network that stores the info about other hosts in internet. This information helps the invaders to recognize those vulnerabilities.
- Topological worms collect the information and form the path to damage via structure of the network.
- The web search worms recognize and determine its target information by search engines.

4.4.2 Propagation Strategy

After the target is identified by the initial worm, the worm spreads copies of itself to other victims through various schemes [13][14] . Self-carried, second channel and Botnet schemes are propagation scheme of worm. The self-carried worms are straight forward propagation scheme. Second channel worms spread from the backdoor or through backdoor of the infected systems. The worms spread through the Second Channel that causes the network using their botnet propagation, where botnet propagation produces strange behaviors by different protocol implementation.

4.4.3Transmission Media

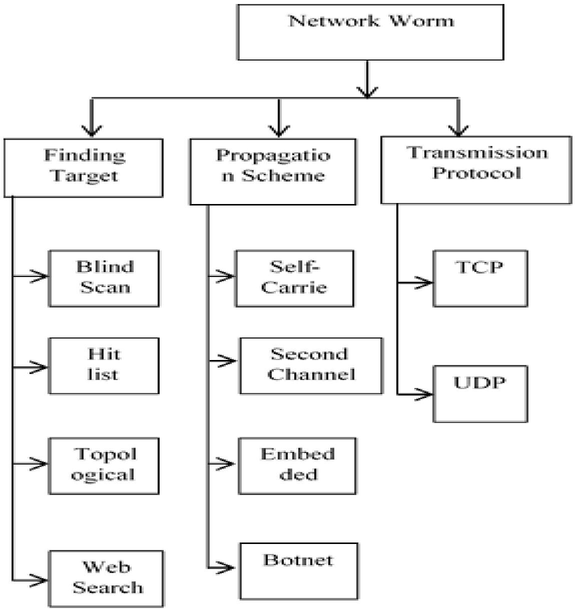

Figure 4.1 Characteristics of worm attacks

Transmissions of worms are performed through Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) worms [13]. TCP worms are connection oriented and latency limited. These worms block the progress thread. UDP worms infect through self-carried. They are connectionless and bandwidth limited. UDP worms block resources in the network.

4.5 Classification of worms

The worms are classified into following classes depending on their severity [13].

- Fast spreading worms
- Highly destructive worms
- Specially targeted worms
- Remotely controlled worms
- Heavily armored worms

4.5.1 Fast spreading worms

Fast-spreading worms cause widespread congestion that will bring down network services such as e-mail and Web browsing (eg: sapphire worm). This worm consists of a 376-byte payload in a single 404-byte UDP packet. Infected hosts can produce these short UDP packets quickly. Sapphire's spreading strategy is depending on random scanning that selects IP addresses at arbitrary manner to infect and finally verdict all susceptible hosts. Random scanning worms originally propagate exponentially at rapid speed. This infection of new hosts becomes less vulnerable because worm uses more time to retrying addresses that are either previously infected or immune.

4.5.2 Highly destructive worms

This type of worms maximized their damage and wreaked havoc on the computer world. One of the most destructive worms on the Internet was stuxnet. This worm damaged Windows systems through unprecedented four zero-day attacks. It is propagated using affected removable drives, and then uses other exploits and methods such as peer-to-peer RPC to affect and update other systems into the private networks that are indirectly linked to the Internet.

4.5.3 Specially targeted worms

This type of worms is specially attacked the targeted system. The Conficker worm spreads itself via buffer overflow vulnerability in the Server Service on Windows computers. This worm implements a specially crafted RPC request to run the code on the target computer. When it runs on a computer, this worm deactivates a system services such as Windows Automatic Update, Windows Security Center, Windows Defender, etc. It obtains further instructions by connecting to a server and receiving a binary update. It receives instructions that may contain to propagating and collecting the personal information and installing additional malware onto the target computer.

4.5.4 Remotely controlled worms

Remotely controlled software consists of two parts: a light-weight server perform task on the vulnerable machine and runs the commands by its operator. Client perform task on the attacker's machine and controls the server component remotely over the network. Before a machine can be remotely controlled, it must be "infected" by the server component of the agent using various methods by the worms through open inbound channels such as e-mail or Web browsing. The most remotely controlled clients run by sending commands inbound according to their server components thus possess the highest threat to home users.

4.5.5 Heavily armored worms

This type of worms includes Klez (Oct 2001), Bugbear (Oct 2001),Winevar (Nov 2002), Avril (Jan 2003) look for common antivirus processes and stop them, scan hard drive for key antivirus files and delete them and disable antivirus Software. An armored worm tries to prevent analysts from examining its code. The worm may use various methods to make tracing, disassembling, and reverse engineering its code more difficult.

4.6 Detection mechanism to handle worms

There are two types of countermeasures to handle worm attacks. They are traffic-based and non-traffic based counter measures [13].

4.6.1Traffic-Based Countermeasures

To develop these types of countermeasures, simple and sophisticated attack models are considered. Accordingly, countermeasures are developed based on two types of traffic generated by worm attacks. In simple model, a worm attack will create propagation traffic directly. In sophisticated model, a worm attack will try to create probing messages to identify the location infrastructure of the defense system, thereby circumventing the detection. The traffic-based countermeasures consist of the following two components: propagation traffic and probing traffic.

Countermeasure Based on Propagation Traffic:

In order to make it similar to the background traffic and circumvent the detection, the worm attacks adopt the feedback loop-control mechanisms to manipulate the propagation traffic. Since periodic manipulative nature of such worms, the worm propagation traffic and background traffic are different in the time domain. Defense scheme uses the Power Spectral Density (PSD) distribution of the propagation traffic rate and its equivalent Spectral Flatness Measure (SFM) to differentiate the worm propagation traffic from non-worm traffic.

Countermeasure Based on Probing Traffic:

Worm attacks carry out probing traffic in a stealthy manner, e.g., launching low-rate of probing traffic encoded by Pseudo-Noise (PN) codes, develops countermeasures against such attacks. To counteract such attacks, information-theoretical framework is needed.

4.6.2 Non-Traffic Based Countermeasures

The second component is to develop non-traffic based countermeasures against worm attacks. It is critical to identify what types of non-traffic features and their characteristics to develop these types of countermeasures. Non-traffic based countermeasures consist of three parts that is based on worm un-controllable features such as dynamic signature of worm program execution, attackers' contradicted objectives and the defender's reputation.

Countermeasure Based on Dynamic Signature:

This detection approach is based on mining dynamic signatures of worm program at run-time executions for new unseen worm attack. The approach allows for the capture of dynamic behavior of executable and provides accurate and efficient detection against both seen and new unseen worms. A large number of real-world worms and benign executable and trace their system calls. Through mining the signatures from the various extracted features in the system call traces, apply learning algorithms for detection. Further, learned classifiers are applied for rapid worm detection with low overhead on the end-host.

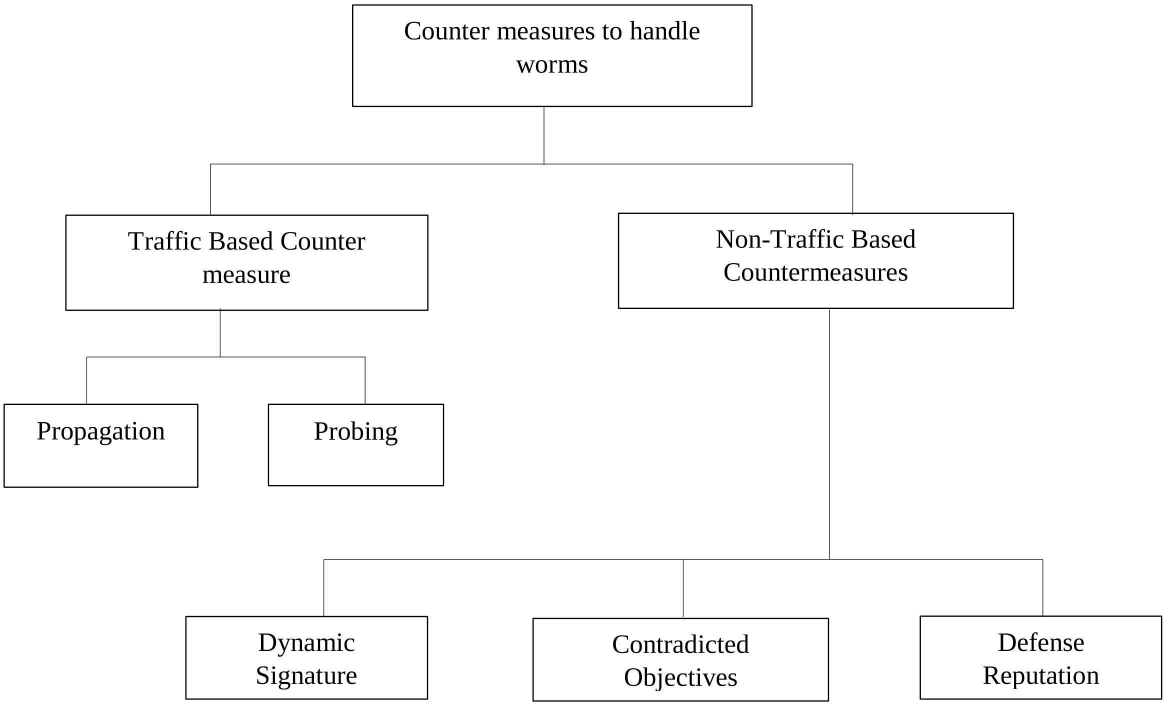
Counter measures to handle worms
Traffic Based Counter measure
Non-Traffic Based Countermeasures
Propagation
Probing
Dynamic Signature
Contradicted Objectives
Defense Reputation

Figure 4.2 Counter measures to handle worms

Countermeasure Based on Contradicted Objectives:

Worm attack becomes smarter and manipulates features used by counter measures. No matter how a worm attack changes strategies, worm cannot change its objectives. Based on this, novel non-traffic based countermeasure is used by testing non-traffic feature like contradicted objectives which guard against worm attacks. Countermeasures are required to propose against self-adaptive worms that adapt their propagation patterns to decrease the probability of detection and ultimately affect the number of computers. To develop countermeasures, game theoretic formulation is modeled to interaction between the worm propagator and the defender.

Countermeasure Based on Defender's Reputation:

Real-world system settings with multiple incoming worm attackers cooperate by sharing their interactions history with the defender. The countermeasure is needed that is based on defender's reputation establishment of toughness in its repeated interactions with multiple incoming attackers. The iterative attacks may allow an attacker to know from previous interactions. The defender use benefit of the iteration by sacrificing short-term performance in the initial few rounds to begin a "tough" reputation.

To counteract such worm attacks, there are two significant steps needs to perform: worm detection and post-detection migration. Worm detection aims to identify worm propagation on the Internet. Once a worm is detected, the post-detection migration techniques can be deployed to slow down and even stop worm propagation. The most commonly used migration strategies such as blocking or filtering propagation traffic and vaccinating the vulnerable computers.

Year	Authors	Methods	Parameters used	Observations
2008	Sellke et al [15]	LPS Worm Containment System	Time deployment	Worm dies out completely in 750 minutes. LPS worm containment system is very effective when there is a 100 percent deployment. When there is only a partial deployment, it protects the local networks and provides global benefit.
2010	Guangsen Zhang et al [16]	Cooperative Internet worm containment and gossip based aggregation	Time	Containment of worm propagation is acceptable even for a gossip interval of 10 minutes.
2012	XufeiZheng et al [17]	Cloud based benign Re-WAWmodel	Time	Slows down containment trend after the switching time of 31.8 seconds but does little effect on the overall containment.
2012	Liming Zheng et al [18]	Malicious packets blocking algorithm	Time	The computational complexity of blocking is O(M+1).Scale to high-speed networks but error comes from that since some normal packets also uses the feature value identified as malicious.
2012	Fabio Soldo [19]	Optimal Source-Based Filtering	Containment Rate , communication overhead	This reduces the collateral damage significantly, i.e., by 50%., while the communication overhead increases only linearly with the overall number of filters available.
2013	Rrushi et al	Botnet Containment	Time	It detects a botnet outbreak at its very early stage, thereby it can enable a timely botnet containment

Table 4.2 Containment approaches of worm

4.7 Containment approaches

The containment approaches are required to block the worms and protect the network from further infection. Various existing methods for containment of worms are discussed below in table 4.2.

5. CONCLUSION

In this recent world of Internet, it is important to secure the data from the security threats like worm attack. During the past 20 years, Internet worms have caused serious infection on the network and heavy financial losses worldwide. This survey investigated security threats to wireless network, various categories of worm, their vulnerabilities and detection techniques are discussed.

REFERENCES

[1] Oona A. Hathaway and Crootof, Rebecca, “The Law of Cyber-Attack”, Faculty Scholarship Series. Paper 3852.

[2] Bryan Watkins, “The Impact of Cyber Attacks on the Private Sector”, Association for International Affairs, August 2014.

[3] WannaCry ransome ware, file:///C:/Documents%20and%20Settings/CLDC%20PAPER/Desktop/2017May-WannaCry-Ransomware.pdf

[4] Dr. P. K. Sahoo and Nikhila Vinjamuri, “Digital Forensic a Novel Way to Investigate ECrime”, International Journal of New Innovations in Engineering and Technology, Volume 5 Issue 4– August 2016, pp. 11-16.

[5] Dr.G.Padmavathi and S.Divya, “A Survey on Various Security Threats and Classification of Malware Attacks, Vulnerabilities and Detection Techniques”, The International Journal of Computer Science & Applications (TIJCSA), Volume 2, No. 04, June 2013, pp. 66-72.

[6] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, “Wireless Network Security: Vulnerabilities, Threats and Countermeasures,” International Journal of Multimedia and Ubiquitous Engineering, Vol. 3, No. 3, July 2008, pp.77-86.

[7] Robert Moskovitch, Yuval Elovici, Lior Rokach, “*Detection of unknown worms based on behavioural classification of the host*”, Elsevier, Computational Statistics and Data Analysis, Vol. 52, No. 9, 2008, pp. 4544- 4566.

[8] S.Divya and Dr.G.Padmavathi, “Computer Network Worms Propagation and its Defence Mechanisms: A Survey”, *Proc. of Int. Conf. on Advances in Communication, Network, and Computing, CNC, pp. 643-652.*

[9] Andhika Pratama, Fauzi Adi Rafrastara, “Computer Worm Classification”, International Journal of Computer Science and Information Security, Vol. 10, No.4, April 2012, pp.21-24.

[10] Vishrut Sharma, “An Analytical Survey of Recent Worm Attacks”, International Journal of Computer Science and Network Security, Vol. 11, No.11, November 2011, pp.99-103.

[11] Ossama Toutonji and Seong- Moo Yoo, “*Passive Benign Worm Propagation Modeling with Dynamic Quarantine Defense*”, KSII Transactions on Internet and Information Systems, Vol. 3, No. 1, February 2009, pp. 96- 107.

[12] Manish Khule, Megha Singh, Deepak Kulhare, “*Enhanced Worms Detection By NetFlow*”, International Journal of Engineering and Computer Science, Vol 3, Issue 3, March 2014, pp. 5123- 5127.

[13] Yong TANG, Jiaqing Luo, Bin Xiao and Guiyi Wei, “*Concept, Characteristics and Defending Mechanism of Worms*”, IEICE Transactions on Information and Systems, Vol. E92- D, No. 5, May 2009, pp. 799-809.

[14] Dr. Divya Midhunchakkaravarthy, “An Efficient And Secure Detection Of Internet Worm Using Propagation Model”, International Journal of Innovations in Scientific and Engineering Research, Vol.3, No.1, JAN 2016. Pp. 8-15.

[15] Sarah H. Sellke, Ness B. Shroff, and Saurabh Bagchi, “*Modeling and Automated Containment of Worms*”, IEEE Transactions on Dependable and secure Computing, Vol. 5, No. 2, April- June 2008, pp. 71- 86

[16] Guangsen Zhang, Manish Parashar, “*Cooperative detection and protection against network attacks using decentralized information sharing*”, Springer, Cluster Computer, Vol. 13, No. 1, 2010, pp. 67- 86.

[17] Xufei Zheng, Tao Li, Yonghui Fang, “*Strategy of fast and light-load cloud- based proactive benign worm countermeasure technology to contain worm propagation*”, Springer, Journal of Super Computer, Vol. 62, No. 3, 2012, pp. 1451- 1479.

[18] Liming Zheng, Peng Zou, Yan Jia, Weihong Han, “*Traffic Anomoly Detection and Containment Using Filter- Ary- Sketch*”, Elsevier, 2012 International Workshop on Information and Electronics Engineering(IWIEE), Procedia Engineering, Vol 29, pp. 4297- 4306.

[19] Fabio Soldo, Katerina Argyraki, Athina Markopolou, “*Optimal Source- Based Filtering of Malicious Traffic*”, IEEE/ ACM Transactions on Networking, Vol. 20, No. 2, April 2012, pp. 381- 395.