IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Review: Computer Worms

Ankur Singh Bist
Govind Ballabh Pant University Of agriculture And Technology, India
ankur1990bist@gmail.com

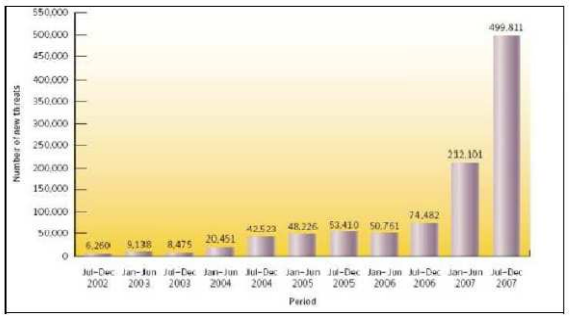
Abstract

This paper presents various approaches and analysis that describes the terminology for computer worms . There are various methods used to detect the computer worms and still lot of work is going on in this direction . Our purpose in this paper is to analyse the various basic terms and defence methods that have been introduced .

Keywords: Computer worms, Payload.

Introduction

Computer worms can be defined as a programs that can have the process of self propagation . There are various process that have been used in the direction of classification of worms from normal files that will finally lead to worm detection . Machine learning techniques are widely used in this direction . As statistics says that the attacks of malicious codes are increasing day by day so there is requirement of strong techniques that can be used for their detection. Worm designers or in total we can say malicious code designers use lot of techniques that are difficult to analyse and detect . The static methods also seems not to work in the case where every time there are rapid dynamicity from attacker side so now a day's main focus is going towards the methods that are dynamic and are able to detect zero day worms .



Malicious Threat Rise

The rise in the malicious threats like computer worms activities are required to be handled and observed strongly to make certain defence that can stand as a saviour of security domain. Other type of malware are:..

1. Viruses
2. Trojan horse
3. Botnets
4. Adware
5. Spyware

Elements of Computers Worms WORMS

Human activation , human activity based activation , scheduled process activation ,self activation are the different ways by which worm is activated on host . There are following ways adopted by the worms to find the target machine that is to be infected[2] -

1. Scanning
2. Pre-generated target lists
3. Externally generated target list
4. Internal target lists
5. Passive

A worm can propagate in various forms like [2]-

1. Self-Carried
2. Second Channel
3. Embedded

The code that is carried by the worm and in which routines related to propagation are not included is payload that can be seen as [2] ---

1. Nonfunctional
2. Internet remote control
3. Spam relays
4. Html proxies
5. Internet dos
6. Data collection
7. Access for sale
8. Data damage
9. Physical world remote control
10. Physical world DOS
11. Physical world Reconnaissance
12. Physical world damage
13. Worm maintenance

The attackers make worms due to various reasons [2]-

1. Experimental curiosity

2. Pride and power
3. Commercial advantage
4. Extortion and criminal gain
5. Random protest
6. Political protest
7. Terrorism
8. Cyber warfare

Thus the whole activity of worm or in global way we can say that malicious code designer is to create a harm or threat to society so this should be prevented. There is need of creating better methods to fight .Prevention is always better than cure so there are various prevention measures that an end user can take to save their systems .

There are various methods that has been used to detect worms basically this problem hat want to find that the certain file is infected or not is NP . Still there are lots of effort done by authors that are involved in the direction to solve this problem researchers from every field like artificial intelligence , data mining , cryptography and other gave their ways t solve this problems , but still no one have reached to complete solution every time fight turns harder and harder since worm designers are creating more dangerous worms . There are various soft computing techniques that are used in this domain . Neural networks , genetic algorithms helped a lot in this direction with this there are lot of classification algorithms that are used[3] -----

1. Decision tree
2. Naive Bayes
3. Bayesian networks
4. Artificial neural networks
5.

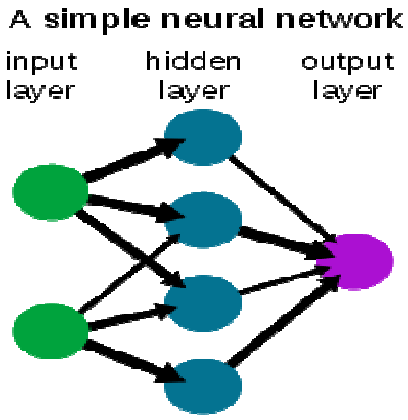


Fig . neural network [1]

Among all neural networks are widely used , the neural networks are basically used to solve the classification problem . In our case the problem get converge o classification problem since the main motto is to make separate the worms from normal files for this task first of all a training data set is needed to train the neural networks once the data set is prepared then the next step is to make the training process the data set used for training must be in proper range and the ways to select features is also essential to observe . Feature selection methods are as follows[3] -

1. Chi square
2. Gain ratio
3. Relief

After the good training finally now tested data is used for creating and maintaining the required analysis in this process one factor is optimization for that various algorithm used like-------

1. BFO
2. PSO
3. SIMBO

These are the recent algorithms that are used for optimization in which SIMBO is latest one that is to be used in new experiments regarding new positive results . Particle swarm optimization is also good algorithm that has been used in so many cases till now .The other classification methods like decision tree and other are very important and show good results but what matters now the best result as produced by combinational mechanism of various entities or by individual performance shown by various entities in this domain. The advance methods used the various classification technique classification techniques that are derived from artificial immune system process and other like the pattern of system calls o make their analysis .The another algorithms that have been used ----

1. Clonal algorithm
2. Positive selection algorithm
3. Negative selection algorithm
4. Dendritic cell algorithm

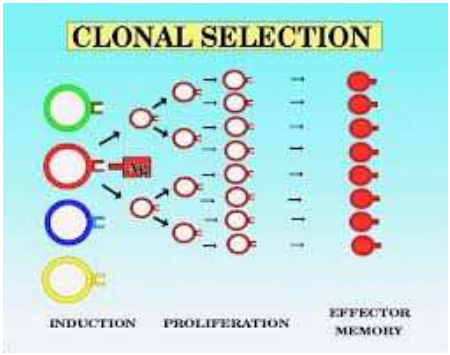


Fig. Clonal selection [1]

Event based techniques that observe program behaviour-

1. User mode API hooking
2. Kernel mode API hooking

3. Kernel mode callbacks

Followings factors are try to make find by the researchers –

1. Measuring accuracy of algorithms
2. Proper selection of features
3. Measure of various computer activities
4. Detection accuracy for known and unknown worms

Conclusion

In this paper basic terminology related to computer worms get discussed . Various methods and approaches related to worm detection get discussed to make the further analysis simpler .Methods of soft computing and optimization techniques are widely used for various problems and in this domain these solutions also play good role.

References

[1] www.wikipedia.com
[2] Nicholas Weaver , Vern Paxson ICSI , Stuart Staniford ,"ATaxonomy of computer worms "