Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

A Study on Malware Detection and Analysis Method

Arish Venkat.M.B*, Manoj Kumar.N**
*(Student, Department of Software systems, Sri Krishna Arts and Science College, Tamil Nadu, India.
Email: arishvenkat2000@gmail.com)
** (Student, Department of Software systems, Sri Krishna Arts and Science College, Tamil Nadu, India.
Email: manoj1035manoj@gmail.com)

--************************----------------------------------

Abstract:

Today most probably malware attack is most common issues in the system and network organization. This threat is spreading very fast to every system by the means of network band in the means of hacking them easily. This main cause is fetching of information without users knowledge. In the past decade there are many malware attack happened by hacking the system. There are some futures to fetch them without knowledge, for example virus is the commonly known malware attack which happens every day. Virus is attacked by share a file from the host, in that file there is simple sort of code attached back side of the file, once that file is inserted and opened by the user the system will be affected with virus. Nowadays not only through virus malware attacks there are different kinds of malwares available, it purely depends on the editor. These malware can be detected with some of the detection methods for example signature and behaviour based technique. So in this paper you can be able to know about malware and its detection methods.

Keywords-**malware, types of malware and detection methods.**

--************************----------------------------------

I. INTRODUCTION

Malware is also known as malicious software which is used to hack or damage others computer system without the users anonymous. There are various types malware few are virus, worms, spyware [10], adware and Trojan horse. Malware can be obtained by any ways using these kinds of malware types. This malicious software executes when a host sends the file or web application with a simple code. Malware is created in the early 1980's [1]. First the malware is created to spread virus in the computer to fetch the data for their known purpose or business sectors for the other company's secret information. This is most dangerous virus in the day to day's life. This can also be spread over internet websites or webpage, when you open that page there will be some sort of code behind the web it is invisible to the user only the hacker can view, once you open it the system will be hanged or hacked through means of network. It is equal to cyber attack which can't be easily found by any one. This kind of software is illegally banned by the government. For such kind of case they have introduced cybercrime. Those data's which is been steeled or fetched from other user depends upon creators imaginations. This creator may also demand by payment methods like fetching the secret data from a important person or companies which has higher amount of income, from them creator used to get money by black mailing them by using with the help of data which was stolen from the person. Sometimes they target government or corporate websites for secret information. The hacker writes the program in a sort or simple way which is invisible to the user and attaching them with the file, after that is created the host sends it to the person in anyway then the user opens it virus attacked to the computer OS. This can cleared only after it is them before it is been affected. The writer creates in different ways to fetch data like they can scan all incoming network data over internetwork broadband and does not allows the information it comes across the page. These codes are first written for pranks. Since these are used for business profits. Some hackers create an app inside that there will be invisible code used for hacking your system or mobile once opened. These activities are done not by an amateur person, only by sophisticated person can to this work.

II. MALWARE DEPLOYMENTS

There are many types of malwares available in today's world. Malware comes in various forms and categories [4]. These are used according to their action which it depends on the machine. Each attack it different from each other, one will be easily attack other one will be difficult. Some type of malware can be easily removed by the user with the help of antivirus software. Only few malware types cannot be protected by the user. Some of the most important malware types are explained below.

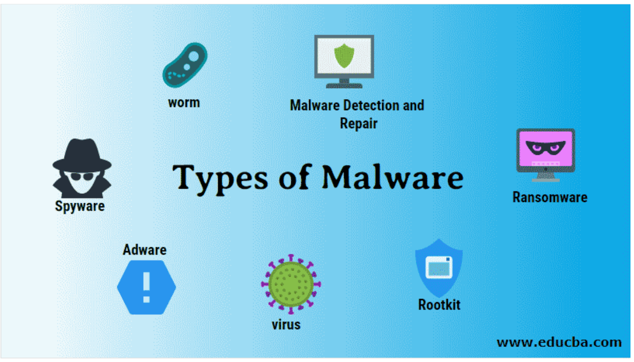

Fig.1 Types of malware

A. Virus

Virus is a dependent malware attack which happens without user's knowledge [1]. This is done by using with the help transferring a file or document. From that file the hacker can insert the virus using an invisible code which will be harmful action [2]. Virus can also be sent by a PDF or JPEG format. While opening the document or file the system will affect by the virus, some of your data will steeled and the system will be hanged. Researchers are finding a anti-virus software for detecting the virus. Normally in every system there will be antivirus software available for protecting their computer system. While using these apps it may clear some virus attacked to the system. This may also be caused by transferring from one computer to another computer. Virus is basic malware attack happen each time, without the user's identity. Once virus is attacked the whole system will be in a collapse manner.

B. Worms

Worms is independently accessed malware attack, which spreads over network based connections. Worms are caused to network like sending by emails, documents or file protocols over internet connections. In other way by opening a webpage or website it can be attacked. The writer writes the code according their mind set. Meanwhile hackers crack the website like pornography or some unwanted images, after viewing that the system can be easily hacked by them and the data can fetched easily. Likewise the hackers can hack the webpage of the government or business sectors page for steeling the secret data information's. Both worms and virus cause “payload” [1]. The worms are differing from virus because worms can be easily sent but virus can't do so. It can be spread in a different ways [3].

C. Trojans

The term Trojans is derived from Ancient Greek word, which spread over system OS. Trojans first affects the system OS, so that it can be easily fetch data. For example if a user sends an email to you, when you open it the system automatically hacked. Sometimes Trojans is also called as Trojans horses. This Trojans is created at backdoor step on your computer, so the data's can be steeled by third party. This may also focus on banking transactions for steeling of money. Sometimes this method is affected by means of clicking advertisement and sending applications for OS, using that data's can be easily fetched. Trojans also affects the software used in the system. Normally the hacker sends link from that it can be easily fetched information. Trojans mask themselves by appearing to be something legitimate [4]. This is the most unpredictable malware attack.

D. Adware

Adware is a commonly known malware attack which is easily attached and removed by the attacker. It is basically a an advertisement which produces an malware attack, for example in a website will visiting a page hacker hacks the page and displays the screen as an malicious advertisement. But this cannot be stopped by any one. These produces a malware affect to the users device easily. More than virus malware this so simple method but some sort of coding is need for the hacking purpose. This advertisement can be hidden by the user by selecting the report page. This adware is easier to remove. You just need to find the malicious executable file and so it can be easier to remove it.

E. Spyware

Spyware is software which performs to gather information from the users system without their knowledge. Spyware is a tracking device or root which the host can easily track the system with the kind of software they produced in that system. Generally spyware is owned by the user with help of corporate or public sector field computers who will be the host of the hacking so that their system can be monitored. The spyware is a function of simple monitoring [5]. Spyware can collect every data file or database which is shared over internet. Even they can take our personal details and banking accounts for freezing or theft of amount from our account without the knowledge. This spyware is not like applying the code in the file or webpage like virus and worms. Simple method is used by the editor for doing spyware malicious software. Generally malware is other term which can be easily said that spyware, which the information, data file and database of a person is fetched from the computer system.

III. MALWARE DETECTION TECHNIQUES

Malware detection is process were the malicious attack is been prevented before it attacks the computer system. A general use of malware detection prevents loss of information and system compromise [4]. It is divided into two simple techniques traditional and non-traditional techniques. Under traditional techniques signature and behavior method, non-traditional technique heuristic method. These each techniques are described briefly below:

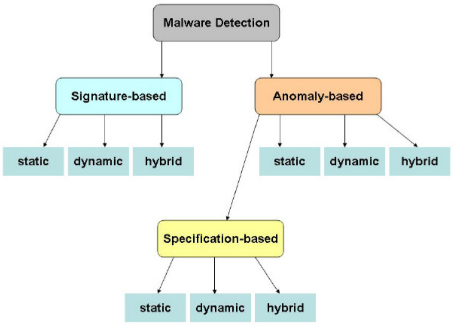

Fig 2. Malware Detection techniques

F. Signature Based Techniques

A signature based technique is pattern system which identifies malware attack before it affects the system. It contains database of recognized attacks and activity is compared with signature database. Signature based system can also be referred as intrusion detection system (IDS) which shows a notification or alarms to the system that malware is been attacked or a virus is inserted to the system. This system is invented in early days with help of cyber security to protect the system from the malware host. This detection can be referred to as Hash based [9]. This method flows in a manner first the file arrives from the other user, anti-virus scanner scans the signature with the already stored patterns and once if it matches it shows the virus notification or else it accepts the signature pattern and allows the file to execute in the system. The hacker can use polymorphism and metamorphism to remove the signature pattern and cause the virus with changed signature. So that in this detection method can also be hacked in a simple manner. In signature detection method finger print is also been used for protection. The signature is applied to the file or document so that only one user can access it and it does not matches the other signature pattern. This signature pattern is also known as Misuse detection [4]. Signature is simple techniques which can be easier to identify the data which has malware attack or not. First signature ID is rectified with the file and then that pattern will scanned with the stored pattern files after that only the files runs in the computer with peaceful manner.

G. Behavior Based Techniques

Behavior detection technique is used for identify whether there is malicious attack in computer system. The behavior based approaches the program to monitor if there is any malware available. This is monitored in the bases of system calls from the operating system [7]. Generally behavior based is also known as Ruled based [9]. Using this technique the malware can be modified easily and unauthorized users can be found. This method has various dangers to the computer like installing root kits, shutting down or disabling system services, downloading and installing unwanted software or application which will harm the system. This behavior observes when software executes to the system and then this method analyses the code if there is a match it will ignore that software. It is not to be depends only on the signature based technique. In this technique there are many sorts of advantages and disadvantages available. This has a separate based method used by cyber security to find the host behind this malware attack. Researchers are finding the advanced behavior method to find the host, from this we can find their id proof and address. This will help the private and public sector companies for protecting their properties using this behavior method. Behavior method recognizes the file whether it has malware or not. It’s generally a security software which protects the system OS from malware. In this software the malicious code rectified by means of pattern or some sorts of matches. This won’t allow unauthorized users inside the computer system. Behavior based techniques can be used by any by downloading the software application to protect.

H. Heuristic Based Techniques

Heuristic technique is used to protect the computer system from unknown computer viruses. Heuristic is a method of detecting viruses by examining cod for suspicious properties**.** Cybercriminal are constantly developing new threats, and heuristic is one of the only methods used to deal with the huge volume of these new threats seen daily. The one method used in heuristic technique static method which analysis the malicious code and rectifies it before used in computer. Heuristic method is used with machine learning and data mining [8]. We have noticed that in signature based and behavior based has disadvantages in it, but in heuristic method those disadvantages are taken into advantages so that virus can be rectified in easier manner. This heuristic method is also referred as anomaly based detection [4]. This mainly focuses on the unknown defect to the system. This is used to find the known and unknown virus defect. This is different from both method of malware detection. Heuristic antivirus programs that utilize heuristic method this function by executing the programming commands of a questionable program or script within a specialized ML. A machine learning model should theoretically be able to make the same detections than a behavior based approach, in much less time on assuming machine learning. This overcame the disadvantage of signature based and behavior based method.

IV. MALWAREW ANALYSIS TECHNIQUES

Before detection method first analysis method should be done to analyze the intentions [6]. This is executed by the code or by using the software to protect and analyze the malicious code. Its main goal is to analyze the malicious code which is attached in the file or document sent from the hacker. This analysis method is used for study the components of malware [2]. There are two analysis techniques to analyze the malware attack they are static and dynamic analysis [9]. Those two methods are described below:

I. Static Analysis

This static analysis is used to protect the system before malware attack. This method first analyzes the file and then executes the file inside the system. This method is also known as code analysis [1]. There are some tools available for analyzing the malicious code detects the computer system some are disassemble tool, decompile tool and debugger. This method can be analyzed with few steps which are used for analyzing the malware. Static analyzer is used to perform the file before executing in the system. This is a useful for the system network also so that it could not be hacked by the host. This is a method of computer debugging that is done by examining the code without executing the program. Some automated tools can examine the assist of programs so that it can be analyzed with the static analysis. Through this static analyzer we can study and go through the information about the malware codes. Static analysis is only a first step in a comprehensive software quality-control regime. So it is easier to analyze the malware and know the hosts needs with this static analysis.

J. Dynamic Analysis

Dynamic analysis is different from the static analyzer because in static analysis analyzes the file before execution, but in the dynamic analyzer after the file executed this method will analyze it. Dynamic analysis is the testing and evaluation of a program by executing data in real time. The most objective in dynamic analyzer is to find error in a program while it is running, rather than by repeatedly examining the code offline. This dynamic analysis is performed and executed with real or virtual processor. This can be done with tracking the instruction [2]. This same as behavior based technique which runs after execution. While static analysis is performed in a non runtime environment, dynamic analysis adopts the opposite approach and executed while a program is in operation. Dynamic analysis finds properties that hold of one or more executions. Dynamic analysis typically instructs program to examine or record some of run time state.

V. CONCLUSIONS

From this paper you will be clearly known about what are the advantages and disadvantages of malware attacks. Day to day malware attack is been spread virally with various types of ways. This attack has reduced somewhat with the help of researchers and cyber security. Some people don't know about this malware attack happens in their system, so this should be taken in a serious way so that people can know about it and they will protect them from virus, adware and other kinds of malware attacks. Various detection is described in this paper, from that you should be able to get how to protect your system from malware attacks. This may help some research people to know prevent and secure in different way to their acknowledgement. This paper will be useful for researcher for their research field. So every people should be safe guard their system so that personal information will not be steeled and hacking the network band to avoid uninterrupted service in the base network.

REFERENCES

[1] A Study on Malware Taxonomy and Malware Detection Techniques
Satya Narayan Tripathy1, S. K. Das2, Brojo Kishore Mishra3, Om Prakash Samantray4
1,2,4Department of Computer Science, Berhampur University, Berhampur, India.
3C. V. Raman College of Engineering, Bhubaneswar, India.

[2] Malware Analysis and Mitigation in Information Preservation Aru Okereke Eze and Chiaghana Chukwunonso E. Department Of Computer Engineering, Michael Okpara University Of Agriculture, Umudike Umuahia, Abia State-Nigeria. Corresponding Author: Aru Okereke Eze

[3] Review of Malware and Techniques for Combating Zero Day Attacks Emmah, Victor Thomas Ejiofor, C. I Onyejegbu, Laeticia N.Department of Computer Science, Rivers State University, Nigeria Department of Computer Science, University of Port Harcourt, Nigeria. Department of Computer Science, University of Port Harcourt, Nigeria.

[4] Malware and Malware Detection Techniques: A Survey Jyoti Landage ME, Dept of Comp Engg Sinhgad College of Engg, Vadgaon, Pune Prof. M. P. Wankhade Professor,Dept of Comp Engg. Sinhgad College of Engg, Vadgaon, Pune.

[5] Spyware and Trojan Horses Sonali Jadha, Department of Computer Engineering Rajashri Shahu College of Engineering, India.

[6] A SURVEY ON MALWARE DETECTION AND ANALYSIS TOOLS Sajedul Talukder1 and Zahidur Talukder2, 1Department of Mathematics and Computer Science, Edinboro University stalukder@edinboro.edu,2Department of Computer Science, University of Texas at Arlington.

[7] Analysis of Signature-Based and Behavior-Based Anti-Malware Approaches Ashwini Mujumdar, Gayatri Masiwal, Dr. B. B. Meshram.

[8] A Survey on Heuristic Malware Detection Techniques Zahra Bazrafshan, Hashem Hashemi, Seyed Mehdi Hazrati Fard, Ali Hamzeh Department of Computer Science and Engineering Shiraz University Shiraz Iran {zbazrafshan, h-hashemi, hazrati, ali}@cse.shirazu.ac.ir

[9] COMPARATIVE ANALYSIS OF MALWARE DETECTION TECHNIQUES USING SIGNATURE, BEHAVIOUR AND HEURISTICS *Odii, J. N. Hampo, J.A.C. Department of Computer Science Dept. of Computer Science Federal University of Technology Federal University of Technology.
Owerri Nigeria Owerri, Nigeria jnodii@yahoo.com hampojohnpaul@gmail.com

[10] A Survey on Malware and Malware Detection System Imtithal A. Saeed Faculty of Computing Universiti Teknologi Malaysia, 81310 UTM Johor Baharu Campus, Johor, Malaysia Ali Selamat Faculty of Computing Universiti Teknologi Malaysia, 81310 UTM Johor Baharu Campus, Johor, Malaysia