ISSN:0975-9646

Monika Agrawal et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3381-3383

Evaluation on Malware Analysis

Monika Agrawal[1], Heena Singh[2], Nidhi Gour[3], Mr. Ajay Kumar[4]

M.Tech Scholar, CSE, JECRC UNIVERSITY,
Jaipur, Rajasthan, India[1, 2, 3]
Assistant Professor, CSE, JECRC UNIVERSITY,
Jaipur, Rajasthan, India[4]

***Abstract*- In this technological era everyone's life is influenced by Internet. It plays an essential role in today's life style and businesses. Sharing information, communication, socializing, shopping, running businesses and many more are now easily achievable by internet. In spite of its vitality, the Internet experiences significant inconveniences, for example, clients' privacy, robbery, fraud and spamming. Viruses are the Internet's number one opponent and today's viruses are more complex then old era. They utilize numerous methods to escape of the anti-virus programs and have a tendency to work silently at the backdrop. Malware, a malicious code seeks financial benefit instead of physical harms and some are handled by expert criminal associations.**

The purpose behind this review paper is to distinguish the techniques and tools utilized by anti-virus to secure Internet's clients from the dangers of malware. Seeing how the malware is constructed and how it is utilized by the attackers is getting essential for system administrators, programming designers and IT security field master.

.

Keywords: Malware, Virus, Keyloggers, Spyware, Trojan horse, Backdoor, Botnet or Bots.

I. INTRODUCTION

Malware is malicious software with malicious intents. It incorporates numerous categories, for example, virus, rootkits, spyware, trojan horses, bots or botnet, backdoor etc. Malware has turned into a serious risk to interconnected PC frameworks for a long time. Some study demonstrates that malware is now a biggest cause of billions of dollars losses. The circumstances are getting more terrible, since malicious code writers are in big profit.

The attackers are focusing on actively striving for more complex and stealthy attack tactics to frustrate malware analysis team. They are motivating forces to quickly create expansive number of new malicious programs also new variants (in the request of thousands or significantly more for every day).

Unfortunately, the existing techniques for malicious code or malware detection are a long way from being satisfactory. This segment gives an overview of current strategies and their constraints. Therefore, the aim of this review paper is on automatic malware analysis and detection.

II. WHAT IS MALWARE?

Malware is basically designed to infect or to infiltrate a user's computer system without their informed consent. Trojan, Worms, Viruses, Spyware and Keyloggers are the categories of malware. At the end of the day we can additionally say Software that "deliberately satisfies the destructive plan of an attacker" is generally referred to as malicious programming or malware. Terms, for example, "virus", "worm" or "Trojan horse" is utilized to characterize malware that display identical malicious behaviour.

A different scenario is occupied by malware to infect other computer systems. A remotely controlled malware which is called bot is used to infect an internet connected system. There is an external entity which is known as bot master control this system remotely. The collection of remotely controlled machines is controlled by bot master and this pool is called botnet.

The botnet is rent out by spammer who misuses these remotely controlled bots to send spam e-mails to the users which contains links to a manipulated web contents. This page, thus, may surreptitiously introduce a spyware component on a guest's system which gathers particular data, for example, Credit card details and other online account credentials. The attackers are now able to misuse this information by buying goods online.

All involved attackers make money at the expenditure of the infected user. With the ascent of the Internet and the number of connected hosts, it is presently feasible for a modern attacker or cyber criminal to infect many hosts within few minutes after releasing the malicious code into the wild. Thus malware can be the most dangerous threat for user's computer system. Further we'll discuss types of malware in the next heading.

III. TYPES OF MALWARE

Various kinds of malicious codes are generated and created to infect the user's computer system. Some of the malwares are:

(i) Virus: Virus is a kind of malware that declare by infusing itself into an alternate project called host program. Infection can influence your framework in a serious manner. The infections are appended to executable files that means a virus can exist in a framework however are not active until and unless the host project is executed. Once the virus-infected program is executed the virus becomes active effecting the folders and files. A virus may harm or devastate information on your workstation framework, or even cancel everything on your hard disk.

(ii) Worm: Worms are self-replicating which uses the computer network to transmit the malicious code to another system. Worms are individual software program that does not require any host program or human involvement to replicate itself to disrupt the data or information.

(iii) Trojan: A Trojan horse is one more type of malware that masquerades or behaves as a useful program with

the purpose of granting an attacker unauthorized access to a user's computer system. Trojan horses are able to replicate themselves, steal the sensitive or confidential information, or damage their host workstation frameworks. Trojans enter the user's systems through installing online games or drive-by downloads, by internet driven applications or by downloading songs or movies in order to reach target user's computer systems.

(iv)Backdoor: Backdoor are the software that permit the hacker/programmer to access the system without utilizing username, password, or any other technique to enter into the system that act as a front door. As its name suggests it is software which allows accessing the computer system from back-door by bypassing the user authentication schemes. Programmer installs the backdoor program which helps them to get into the system without knowing username and password into the login screen.

(v)Spyware: Spyware can collect any type of data including user's personal information like bank account number, credit account number, internet surfing habits, user's password etc. Spyware can gather any kind of information including client's personal information like their bank account details or account number, credit card number or most frequently visited websites and client's password etc.

(vi)Adware: Adware is also sort of malicious software that attempt to offer something to the clients which consequently appear as popup windows even if clients don't open these or even intrigued in these. Normally adware enter to the systems in the form of the gambling advertisements or games format/pop-up windows and these advertisements are the part of websites, which you open.

IV. THE ANATOMY OF MALWARE ATTACKS

An attacker must achieve two goals to infect any user's computer system through web browser.

a. Attacker must find an approach to connect with the user or victim.
b. Attacker need to install malicious code on the victim's computer.

Both these goals will be achieved quickly and without the concern of the user which depends on attacker's tactics.

There is another way to infect a user's system with malware, attacker just simply ask user to visit a website which contains a malicious code while user visit this site his system will automatically get infected by malware.

These days' attackers are focusing on different delivery mechanisms, and usually send malware infected post over social networking sites, such as Facebook.

Other attackers decide to target websites that potential victimized people will visit on their own. To achieve this, an attacker compromises the targeted site and inserts a little piece of HTML code that associates back to their server.

This malicious code can be loaded from anywhere, including a totally distinctive website. Every time a user visits a compromised website in this manner, the attacker's malicious code has a chance to infect user's system with malware.

Variants of Malware

When it comes to detect a malware, we can have our significant focus for the distinctive variants handled or ready exist in significance of the security threats they pose to the computer system.

A detailed discussion about different variants of malware is given as follows:

I. ***Polymorphic Malware:*** A sort of virus is designed to look different every time it replicated, but having the original code intact. This kind of virus is famous as polymorphic virus or malware.

Decryption module is also available with encrypted malicious program in a polymorphic malware. This method of creating polymorphic code is most commonly implemented which uses a generator to transform the code with the original algorithm integral.

A typical execution of polymorphic code is to include encryptor and decryptor with the encrypted malware.

II. ***Metamorphic Malware:*** These are a sort of body-polymorphic, where virus itself transforms from one illustration to another. Metamorphic malware basically use different obfuscation techniques to transform them into a new code which is identical to original code. The metamorphic character of the malware enables malicious program to transform while spreading over the network and making signature based detection absolutely ineffective.

V. MALWARE DETECTOR

Techniques, which are used to detect malicious code or malware, are known as malware detector. Malware detector basically read the malicious code and analyzes the behaviour of this kind malicious code.

There are two types of input that goes into the Malware Detector. They are as follows:

A. Knowledge of malicious behaviour: The detector has the understanding about the difference in normal behaviour and malicious behaviour.

B. Program under inspection: The detector has the program that has to be detected under surveillance.

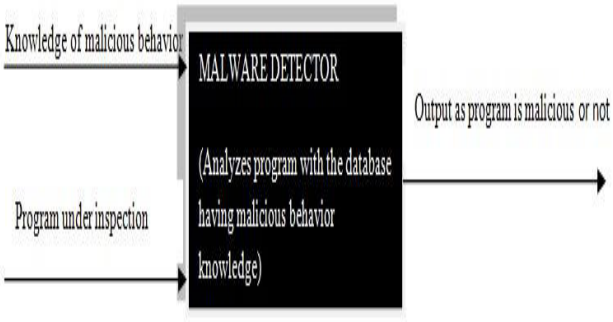

Figure.3. Malware Detector

Above figure defines the functioning of Malware Detector. Malware detector takes two inputs i.e. knowledge of what is considered as malicious behaviour and the other input is program under inspection. Once the malware detector has the idea about the malicious behaviour and compare it with

the code which is in under observation then it can employ whether the code is malicious or not. Malware detector is designed to find out the followings:

(i) False positive: False positive means when the detector finds a virus in a non-infected file. This issue occurs when the bit patterns or signature of file is similar to that of a malware.

(ii) False negative: False negative means when the detector does not find the virus or any kind of threat in an infected file. This happens when the virus is new to the detector or the signature is not in the knowledge of detector.

(iii) Hit ratio: Hit ratio means when the detector is able to find the malware in an infected file. This is because the bit patterns or the signature is present in the database of malware detector.

VI. RELATED WORK

A. ***Malware detection techniques:*** Malware detectors are basically of 3 types:

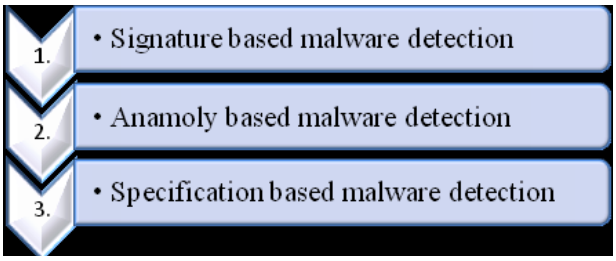

Figure.4. Types of malware detection schemes.

(i) Signature Based Malware Detection:

The signature based malware detection is basically based on the bit patterns contained by malware. This technique generally tries to find out signatures in a code or file which is scanned by the detector to detect virus or threats. A sequence of bytes is known as signature which defines a malware.

Signatures which define malicious code are available in repositories, when any Program under Inspection (PUI) is detected then the detector assess the signature by accessing the repository. If the signature of the PUI matches with signature already exists in the repository then the code will be malicious.

When a developer creates a new signature, he adds this to the repository.

(ii) Anomaly based detection:

Anomaly based malware detection system have two phases. In starting phase the detector learns the normal characteristic. It could be the taking in of the host system or program under investigation or combination of both.

(iii) Specification based technique:

Specification based detection system basically focuses on the requirements for the system or application. In specification based detection system, the starting phase is the accomplishment of some rule set, which specifies the valid behavior any program can exhibit for the system which is being protected or the program is under inspection. The major problem of specification-based detection is that it is often difficult to specify completely and accurately the entire set valid behaviours a system should exhibit.

VII. CONCLUSION

In this evaluation paper we have measured distinctive key issues of malware. We have discussed about malicious code, their effects and detection techniques. Users can be secured by following the protective methods which have discussed above. User must be aware about the malware and their dangerous effects and they should make their system fully protected so the malware can't inject into their system. Conceivable methods are characterized for the protection of the system. This evaluation work is embraced by a portion of the researchers which is in advancement for the planning of the security structure from protecting your system to get infected with malware. For the further improvement the technocrats are basically being actualized so that there ought to be upgrade in the security.

REFERENCES

1. Savan Gadhiya and Kaushal Bhavsar, *Techniques for Malware Analysis*, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE 2013), April 2013.
2. L P. Akyildiz , W. Su , Y. Sankarasubramaniam and E. Cayiric, *Survey on Malware Detection Methods*, IEEE Communications Magazine.
3. Richa Bhatnagar, Mariya Khurshid Ansari, Sakshi Bhatnagar, Harshbardhan Barik, *An Expert Anti-Malware Detection System*, International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-5, November 2012.
4. White Paper, *Malware Security Report: Protecting Your Business, Customers, and the Bottom*, Symantec.
5. White Paper, *The Ongoing Malware Threat: How Malware Infects Websites and Harms Businesses — and What You Can Do to Stop It*, Symantec.
6. Dr. K. Kuppusamy, S. Murugan, "*Preventing Unknown Malware Attack by using Intelligence Intrusion Multi Detection Prevention Systems*, IJCSNS, Vol.9, No. 12, Dec 2009.