ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Analysis on Malware Recognition Methods

[1] J.N Singh
[1] Department Of Computer Science and Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
[1] drjnsingh@Galgotiasuniversity.edu.in

Abstract- Nowadays a malicious program every day is a grave threat. It is created to destroy the computing system, but some of them in the system or data connection is scattered over the linked device.The motive of malware evaluation is to acquire and to provide the necessary data to resolve interference into a system or program. Malicious code or threats is software designed to damage, disrupt or destroy machines, servers, and other related assets. Malware is inserted into devices without its holder's awareness. Servers and mobile devices are really the platforms used for spreading malicious software.Malware always has been a danger to the digital environment, but with the massive increase in internet activity, the malware's effects are becoming serious and it cannot be overlooked. There have been a number of malicious software indicators made; the efficacy of such indicators depends on the strategies used. The paper gives a comprehensive overview on various types of malware and malware recognition methods.

Keywords- Malware, Malware Analysis Technique, Malware Detection Techniques, Types of Malware.

INTRODUCTION

Nowadays Internet usage is perhaps the most important part of everyday life. The Web browser installs various computer program forms. One downside of widespread use is that most computers are susceptible to attack and get malware corrupted.There are various malicious software names, for instance, malicious code, malicious system, or malicious executable[1]. Malware is malicious software that is used in order to violate the security protocols of a software system with regard to privacy, competence and data accessibility.It can attach, alter or delete any software from the process to cause direct harm to the essential functionality of the system. Malware comes in various ways including “Viruses, Trojan horses, spyware, scareware, spyware, trapdoor, etc.”The word malware is brief for "malicious software", as the word implies that malware is meant to attack machines and web users by hiding information, perverting documents, or simply performing malicious operations to irritate customers.Malware spreads widely; it is believed there is a significant increase in information security accidents. Malware hinders system growth[2].Malware attacks the programs running over the web. Since almost all areas of life are using the web to enhance its quality of the service, the need to identify and disable malware as quickly as possible such that the negative consequences produced by such malware can be prevented.Malware is the most considerate threat for embedded systems and the web.Malware is software that allows the system to do anything an attacker wants to do.The identification of malware provides a simple illustration of how to communicate with detecting malicious software.The malware detection system is a scheme used only to identify whether or not software has bad intentions[3].The detection system comprises two functions-analyzing and detecting. Malware Detector is used as a protection instrument against malicious software.Such detectors ' characteristics are defined by the strategies which they use.It requires two parameters first being the signatures or functional specifications of a given code and second being the software being checked, it can use its analysis methodology to assess whether the code is malicious or beneficial.Malware detectors are used to identify such malicious software and virus protection detectors is one of the ways to combat some of these, but with the evolution of malware creation strategies, malware indicators use a variety of methods to escape such program's devastating effect.Artificial intelligence and big data approaches are paired with traditional detection systems to add flexibility in the detection system due to the weakness of current malware detection strategies.Signature-based techniques of identification are nice for identifying recognized malware, but they cannot identify unidentified malicious software and polymorphic malware as they can alter the signatures.Malware attacks programs running over

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

the web. Because virtually every area of operation uses the web to enhance its quality of services, the need to identify and disable malware as quickly as possible such that the negative consequences generated by this malware can be prevented.Malware which has the capacity to propagate are most hazardous since there is no central control, so supporting them isn't a small process.

Types of Malware

Malware occurs in various forms and is widely classified in the preceding groups. They are not exclusive of each other although there are many of them together in one group[4].Malware detection is a complicated process.Apparently malicious is code which allows unwanted access of a device.Malware comes in all forms and in different groups. The various types of Malware is shown below in Fig. 1 Types of Malware

Virus- Through injecting their program into other software, a malicious system spreads from one application to another or from one machine to another. Through copying itself, the virus damage machines and other data.It could not act independently so it connects more specifically exe files and software with the other files and induces network performance loss and denial of service due to its replication functionality; it spreads through files and even machines via the network.

Worm- It is auto-replicating software that transmits copies of itself over a system without user permission from one device to another.Worms are independently-existing malevolent pieces of software.They have a duplicate attribute to themselves.They spread via storage systems and messages, and also utilize system and machine resources that lead to efficiency degradation of the network.As they can make numerous versions of themselves, because of different life existence virus protection detectors can recognise such codes.

Trojan Horse- Trojan horse acts like valuable software but its intent is dangerous.They do not duplicate themselves but it is transmitted while uploading to a device through web contact.It collects confidential information, monitors user behaviour and can remove and modify or modify data on the device in which they live[5].Trojans disguise themselves as pretending to be a valid thing. Usually, Trojans damage data or try to obtain sensitive information like financial information and credentials.

Spyware- Spyware is any program mounted with no customer understanding of the structure. It is a generic term for program that tracks and collects user private information and directs that data back to the intruder so that the intruder could use the hacked information in some untreatable manner.This usually reaches a process when the free or experimental application is installed and activated on the device without the consent of the consumer, switches the browser configuration or introduces abhorrent antivirus.

Scareware- Scareware is a malware that poses as complimentary or experimental anti-virus software, or any other promotional fraud online.When installing fraudulent encryption software, accessing files or accessing a malicious website, the consumer should download this.It gathers all the data stored on your pc after the operation (financial information, private information) that can be traded to other malicious hackers.

Adware- Adware is a marketing-supported technology that performs, exhibits, or uploads adverts to a pc immediately after malware is mounted or browser is used.In particular, such a strand of code is put to free uploaded code.Every time adware is very irritating because it performs ads on user computers against their consent and interrupts the current progress.

Botnet- A bot is a program that allows an intruder to access an infected computer. A web of scammer / attacker-controlled infected machine performs harmful actions without holder awareness.They can render service threats with denials; submit unwanted messages, stealing data.Independent technology is remotely operated by a botnet.

Cookies- Cookies are in sort of data file and include data that is collected by the browser on a user's computers for long term use. Obviously cookies are not dangerous but they become a danger when used by certain spyware.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

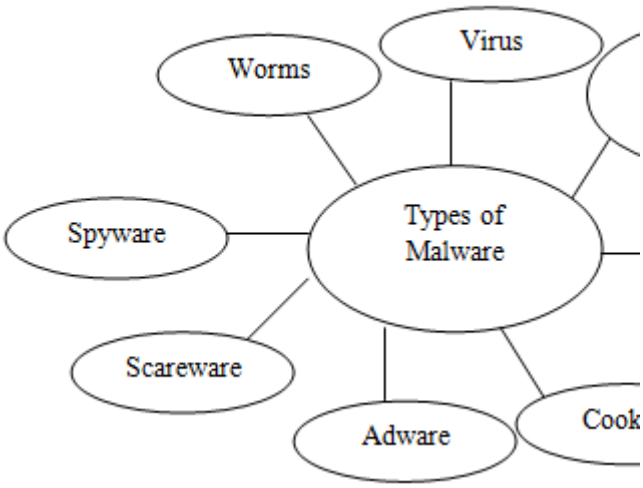

Fig.1: Types of Malware

MALWARE ANALYSIS METHODS

Malware analysis represents a phase towards the identification of malware.To identify malware, first, we need to examine how malware performs its task and what the intent behind malware creation is to make it simple for malware predictor designers to enforce the protective features[6]. The different types of Malware Analysis Techniques are shown below in Fig. 2 Malware Analysis Technique.

Static Analysis- This type of evaluation is called static analysis or code analysis if a programming or piece of software is examined without performing it.Historical data is taken from the software to assess whether or not the program involves malicious software.In this approach, the program is reprogrammed using various techniques and the malicious software design is examined to understand the process.Pre-processor, deceiver, code generator and open source analyser are distinct tools which can be used to conduct static analysis.Static research means reviewing the usable text without the actual instructions being surveyed[7].Static analysis will demonstrate whether a record is damaging, provide data on its utility, and then provide information that will allow one to build simple system labels.Static analysis is transparent and can be quick, but they are relatively inappropriate against sophisticated malware and may lose essential procedures.

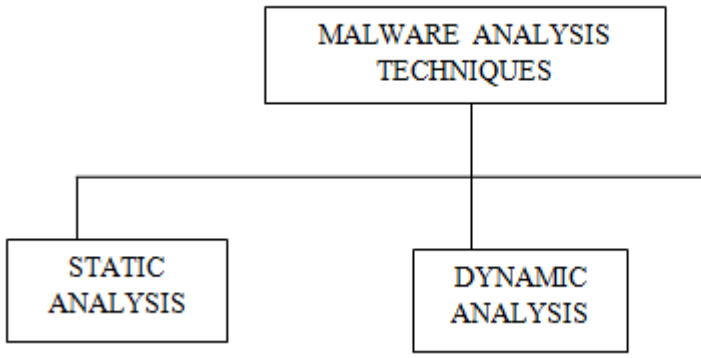

Fig.2: Malware Analysis Techniques

Dynamic Analysis- Techniques of dynamic analysis involve executing the malware and monitoring its actions on the system to end damage, produce positive points, or both.Until anyone can run malware safely, it should build up a scenario that will allow us to focus the malware operating without any risk of injury to the structure or device.In a virtual world, malicious software is run to track the actions and layout behaviour against those unhealthy behaviours.The instruments used to analyze dynamics are "sandbox, simulator, RegShot emulator, Process Explorer."The dynamic analysis makes static analysis further efficient as in this methodology; the contaminated program is performed for tracking reasons in virtual machines.Dynamics analysis can reliably detect other types of malware.Such a type of analysis takes longer as there is a need to develop the environment to perform a malicious code and to test it.

Hybrid Analysis- This incorporates methods of static and dynamic analysis so that both strategies can take advantage of the benefits. First, by verifying the signatures of the malware a program is analysed by code review and it is then operated in a simulated environment to analyse its current behaviour[8].

MALWARE DETECTION METHODS

Malware detection methods are used to identify the malicious software and prevent infection of the computer network, shielding it against possible data loss and device breach[9]. They may be classified into “signature-based detection, behaviour-based detection/heuristic based detection, and specification-based detection.”

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Signature based Detection- When a malware is created, a series of bit usually known as a signature is inserted in its software that can subsequently be used to classify to which group the malware belongs.Many virus protection systems employ the signature-based detection method.The antivirus software disassembles the compromised software code and searches for a sequence that belongs to a community of malware..signatures of malware are kept in the repository and used in the identification phase for comparison. That sort of identification strategy is also known as searching or matching series or sequence.This preserves the signature sample and identifies malware by comparing the sequence to the repository.Such signatures are generated by looking at the partially assembled discrete malware software.Partially assembled software is examined, removing functionality[10].The key benefit of such an approach is that it can reliably detect recognized malware examples, it takes less time to detect the malware and it focuses primarily on the signature of the threat.The biggest disadvantage is that it cannot identify the latest, unidentified malware cases since there is no signature accessible for such malware sort. The Signature based Malware Detection technique is explained below in Fig. 3 Signature based Malware Detection

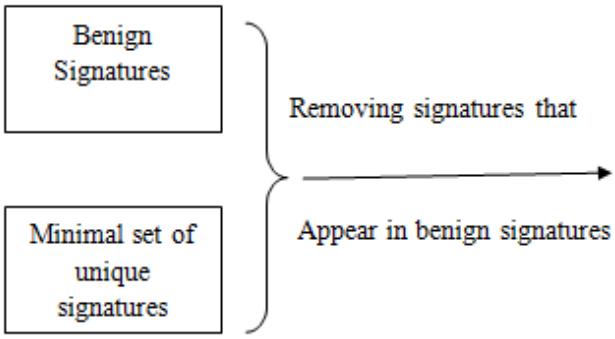

Fig.3: Signature Based Malware Detection

Behaviour Based Detection- This is also referred to as heuristic or anomaly-based detection. The primary aim is to examine the conduct of identified or unidentified malware. The behavioural variable involves different aspects like as malware origin or target address, attachment types, and other quantitative characteristics that are measurable.This typically occurs in two phases: the training phase and the detection phase[11]. In the training process, device activity is detected in the absence of threat and machine learning methodology is used to make an account of such normal behaviour.Such a profile is measured in the detection process against the actual behaviour and variations are marked as possible attacks. The main components in this technique are-

- Data Collection- Such element gathers the knowledge both dynamic and static.
- Interpretation- Transforms the raw information obtained through the framework for data collection into indirect depictions.
- Matching Algorithm- It is used to equate interpretation with a behaviour signature.

The benefit of such an approach is that established as well as recent, unidentified occurrences of malware can be identified and it relies on device actions to identify uncertain attacks.The drawback of such a method is that the information defining the conduct of the structure and the stats in ordinary profile has to be updated but it continues to be big.It needs further resources such as CPU time, storage and disk storage and high levels of adverse events. The Behaviour based Malware Detection Technique is shown below in Fig. 4 Behaviour based Malware Detection

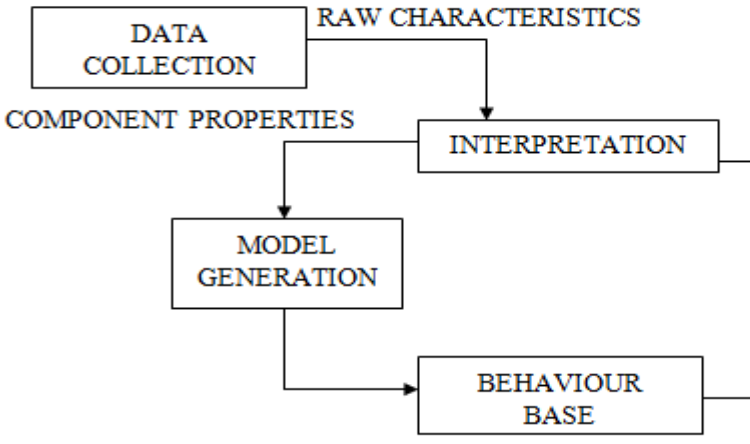

Fig.4: Behaviour Based Malware Detection

Specification based Detection- It is a behaviour-based identification variant that aims to surmount the regular high false alarm frequency correlated with it. Specification-

based detection is based on software requirements that define the safety-critical programs expected behaviour.It requires tracking system executions and identifying divergence from the configuration of the activity, instead of identifying the incidence of different patterns of attack. The approach is similar to anomalies identification but the distinction is that rather than depending on artificial intelligence algorithms, it will be dependent on carefully created requirements capturing valid device behaviour.The benefit of such a strategy is that it can identify external and internal cases of malware, and the rate of false positives is small however the rate of false negatives is large and not as successful as behaviour-based identification in identifying major threats; particularly in system testing and denial of service.Requirements are tracked as per their requirements in specification based detection strategy and tests for objective and subjective behaviour.Still, such approach is a direct analysis of certain program's usual activities. It solves the disadvantage of heuristic-based strategies by raising false-positive levels and growing false-negative levels.

CONCLUSION

The web industry is booming increasingly, consumers and organisations need internet-based safe and comfortable operations. Malware is a serious threat to the customer's computer system in terms of obtaining sensitive information, perverting or destroying the safety system. Today the danger of malicious software has risen several times over, with simplicity in the distribution of resources and technical skills as to how new malware is developing each day with the aim of not being identified.There is a need for a method to safeguard vital information, data privacy that enables in the assessment of malware on side and manages to keep the customer protected from similar efforts by giving necessary support.Malware is passed to machines without its customer's awareness. Mostly the mechanism used to propagate malware is routers and handheld devices. The aim of malware detection is to acquire and to provide the necessary information to address a system or system invasion. The paper gives a detailed overview on malware detection techniques, the types of malware followed by various malware analysis techniques.

REFERENCES

[1] S. Furnell and J. Ward, “Malware,” in *Information Security and Ethics*, 2013.

[2] G. A. N. Mohamed and N. B. Ithnin, “Survey on Representation Techniques for Malware Detection System,” *Am. J. Appl. Sci.*, vol. 14, no. 11, pp. 1049–1069, 2017.

[3] J. Landage and M. Wankhade, “Malware and Malware Detection Techniques: A Survey,” *Int. J. Eng. Res. Technol.*, vol. 2, no. 12, pp. 61–68, 2013.

[4] V. S. Subrahmanian, M. Ovelgönne, T. Dumitras, and B. A. Prakash, “Types of Malware and Malware Distribution Strategies,” 2015.

[5] N. Lord, “Common Malware Types: Cybersecurity 101,” *Veracode*, 2012. .

[6] R. Sihwail, K. Omar, and K. A. Z. Ariffin, “A survey on malware analysis techniques: Static, dynamic, hybrid and memory analysis,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, 2018.

[7] B. Dondogmegd, U. B., and N. J., “A Malware Analysis Using Static and Dynamic Techniques,” *http://www.sciencepublishinggroup.com*, vol. 5, no. 1, p. 20, 2015.

[8] A. Damodaran, F. Di Troia, C. A. Visaggio, T. H. Austin, and M. Stamp, “A comparison of static, dynamic, and hybrid analysis for malware detection,” *J. Comput. Virol. Hacking Tech.*, 2017.

[9] P. G. Shinde, P. D. Motwani, and P. V. Shinde, “Survey on Malware Detection Techniques,” *Int. J. Mod. Trends Eng. Res.*, pp. 74–79, 2015.

[10] J. Scott, “Signature Based Malware Detection is Dead,” 2017.

[11] R. Mosli, R. Li, B. Yuan, and Y. Pan, “A behavior-based approach for malware detection,” in *IFIP Advances in Information and Communication Technology*, 2017, vol. 511, pp. 187–201.

[12] S Balamurugan, RP Shermy, Gokul Kruba Shanker, VS Kumar, VM Prabhakaran, “An Object Oriented Perspective of Context–Aware Monitoring Strategies for Cloud based Healthcare Systems”,Asian Journal of Research in Social Sciences and Humanities, Volume : 6, Issue : 8, 2016

[13] S Balamurugan, P Anushree, S Adhiyaman, Gokul Kruba Shanker, VS Kumar, "RAIN Computing: Reliable and Adaptable Iot Network (RAIN) Computing", Asian Journal of Research in Social Sciences and Humanities, Volume : 6, Issue : 8, 2016

[14] V.M. Prabhakaran, Prof S.Balamurgan ,A.Brindha ,S.Gayathri ,Dr.GokulKrubaShanker,Duruvakkumar V.S, "NGCC: Certain Investigations on Next Generation 2020 Cloud Computing-Issues, Challenges and Open Problems," Australian Journal of Basic and Applied Sciences (2015)

[15] Usha Yadav, Gagandeep Singh Narula, Neelam Duhan, Vishal Jain, "Ontology Engineering and Development Aspects: A Survey", International Journal of Education and Management Engineering (IJEME), Hongkong, Vol. 6, No. 3, May 2016, page no. 9 – 19 having ISSN No. 2305-3623.

[16] Vishal Assija, Anupam Baliyan and Vishal Jain, "Effective & Efficient Digital Advertisement Algorithms", CSI-2015; 50th Golden Jubilee Annual Convention on "Digital Life", held on 02nd to 05th December, 2015 at New Delhi, published by the Springer under ICT Based Innovations, Advances in Intelligent Systems and Computing having ISBN 978-981-10-6602-3 from page no. 83 to 91.

[17] Vishal Jain and Dr. S. V. A. V. Prasad, "Analysis of RDBMS and Semantic Web Search in University System", International Journal of Engineering Sciences & Emerging Technologies (IJESET), Volume 7, Issue 2, October 2014, page no. 604-621 having ISSN No. 2231-6604.