Global Scientific JOURNALS
GSJ: Volume 10, Issue 8, August 2022, Online: ISSN 2320-9186
www.globalscientificjournal.com

A REVIEW ON DETECTION OF METAMORPHIC AND POLYMORPHIC MALWARE

Hashim Ahmed, Manoj Kalita, Pranab Boro, Arup Gogoi, Jyotismita Talukdar,

Abstract

In recent years, malicious applications are increasing at a very high rate and most of them are hard to detect because of their complex code obfuscation techniques. As a countermeasure to keep our system safe and the internet from such malware, these malicious applications must be detected before they infect a huge network. In recent studies there have been several detection methods are proposed. though detection of malware still has difficulties. Some methods are more efficient and faster in the detection of malware, such as Static-based, signature-based, heuristic-based detection. Meanwhile, For malware which is new and has complicated algorithms, models like behavior-based, call graph, and cloud-based work efficiently. And deep learning and machine learning-based approaches are also good in some known and unknown malware but it's a bit challenging task. However, no such detection method has been made to completely compromise all types of malware. This paper gives a comprehensive study on malware detection approaches and techniques. the main focus of this paper is to lay a helping hand to the researchers and provide a good idea about the latest and most effective detection approaches.

Introduction

In day-to-day life, almost every one of our societies is using the internet for our daily life. This is because we cannot think of our life without the internet as it's nearly impossible to work and perform tasks like online transactions, shopping, e-learning, marketing. As the internet has been advanced and evolving very quickly. Nowadays criminals mostly use the internet to do serious crimes as well rather than in real life. Cybercriminals use mostly malicious software to do a cyber-attack on a victim's machine and executing this software intentionally is called malware. There's a variety of computer malicious software for example viruses, ransomware, Trojans, worm, spyware, botnet, rootkit, etc. These applications are designed in such a way that they can infect the victim's machine with contrasting ways to steal their confidential data. With the advancement of technologies, there had been an advancement in the field of cyber threats as well. And one of the most renowned threats is malware. It's software which can disrupt the performance of our personal computer. This malware could be used to harm a user in many ways which include stealing personal data, spying credentials, malfunctioning the device, etc. And with time metamorphic malware has come into existence, which is malware having the ability to change itself through various obfuscation techniques. Here in this paper, we are talking about the two main categories of malware - Metamorphic and polymorphic malware. These two types of malware are very hard to detect as earlier malware was written simple way but nowadays because of their code obfuscation technique. Below we have proposed a comparison table of traditional and new

generation malware.

Table 1: Comparison table of traditional and new generation malware

Comparison parameter	Traditional	New generation
Implementation	simple	complex
Nature	static	dynamic
Propagation type	.exe	it can be any extension
Presence	temporary	relentless
Deal with processes	a few	many processes
Attack type	general	targeted
Shielding challenge	easy	difficult
Targeted devices	ordinary computers	can be any devices

2. MALWARE DETECTION TECHNIQUE AND ALGORITHMS

It is the process where the contents of a program are investigated and determined if the analyzed program is infectious(malicious) or not. And the process consists of three stages namely:

Malware analysis, features extraction, and classification.

Malware analysis:

We need to analyze the malware in order to understand the content and behavior of the malware. In this process, we can determine the operation of a malicious program. How does malware work, what equipment and systems are involved in malware, what data is corrupted and stolen from malware, these answers are known after the malware analysis. We have mainly two ways to analyze malware: Static and Dynamic analysis.

Static analysis: Analyzing a computer program that is not suitable for computers, means malware, without using it is called static analysis. Includes specific techniques such as byte-sequence n-grams, string signature, control flow graph, opcode frequency distribution, etc. The executables are removed and then decrypted before the analysis is done.

In related work on static analysis, in the paper [19] the researchers work on determining whether an executable is a meta morphic malware or a benign. In the process, they used PE file, DDL, and API call to achieve the result. Then in [37] researchers have done detection of meta morphic malware with a high rate of accuracy by using Opcode graph similarity and linear discriminant analysis. The proposed method is based on Opcode graph similarity. Next in the paper [29] researchers use static analysis to extract API calls to detect metamorphic malware. Then they calculated the API call frequency to generate the feature set. In the paper [15] researchers work on the detection of JavaScript metamorphic malware by using their proposed method. They used the Hidden Markov model and opcode graph similarity to did the research work.

Dynamic analysis: Analyzing the behavior of malware while used in a controlled environment is known as dynamic analysis. Dynamic analysis includes different methods such as information flow tracking, instruction tracking, function call monitoring, AutoStart extensibility points, function parameter analysis, etc. The rate of effectiveness of dynamic analysis is higher than static because it does not require the executables to disperse.

In related work in Dynamic analysis, in the paper [28], the researchers specify how a dynamic report can be analyzed and how to prepare the model that helps in taking a decision in the detection of meta morphic malware. Through the use of PE, DDL, and text mining they get some high valued results. Next in the paper [34] the researchers work on converting a random malware sample into API call graph. This conversion is done with the use of operating system resources that represents nodes of the graph and integrates API calls. Then in [11] the researchers implement the function call graph and the graph is applied to the malware detection problem.

Malware features extraction:

By using data mining techniques, we can remove the features of a malware program. Data mining is a process where new information is extracted from a largely unknown site prior to the process. There is a lot of models like the n-gram and graph models that can be used to create malware features & data sets.

n-gram model: The process to remove malicious computer features that are widely used in many areas and malware detection. N-gram is commonly used to detect malicious computer- programs in sequence-based detection techniques.

Graph-base model: This model is a frequently used method to develop malware features. In this way the system calls are converted into graph G (V, E). where V stands for nodes that identify system calls and E stands for nodes that indicate the relationships between system calls.

Malware classification:

It is the process of assigning a malware program to a malware family. In classifying a malicious computer program i.e., malware, different techniques are used such as machine learning, deep learning, etc. A malware program shares similar features within the family.

Machine learning : Static and dynamic approach are used to detect and classify the malicious application ,

Deep learning : A Deep learning engine is used and at first the executables are extracted then it enter to the engine then it gives the malware report

MALWARE DETECTION APPROACHES

In the last few years, there has been a lot of development in educational courses in detection techniques(malware detection). These days, the signature-based method is

used on a very large scale. It works quickly and effectively against a program that is not good for the computer but does not perform well against a malicious computer program that is new to us. Over time, researchers have used techniques like behavioral, heuristic- approach, and model-checking; and also new techniques like these in-deep learning, IoT-based detection, mobile devices, and, cloud. In each case, the feature removal method is a different one from another. And one works better compared to the other because every method has its own boons and bans. With the help of heuristic, behavior, and model-checking-based approaches a large number of malware programs can be detected having few behaviors and specifications. Also, using these methods, newly generated malware can be easily detected. However, they are unable to detect all malware. It is really necessary to find a way that successfully finds more complex and unknown malware. Now, it contains the details presented a review of the books, as well as the pros and cons of each research, is described.

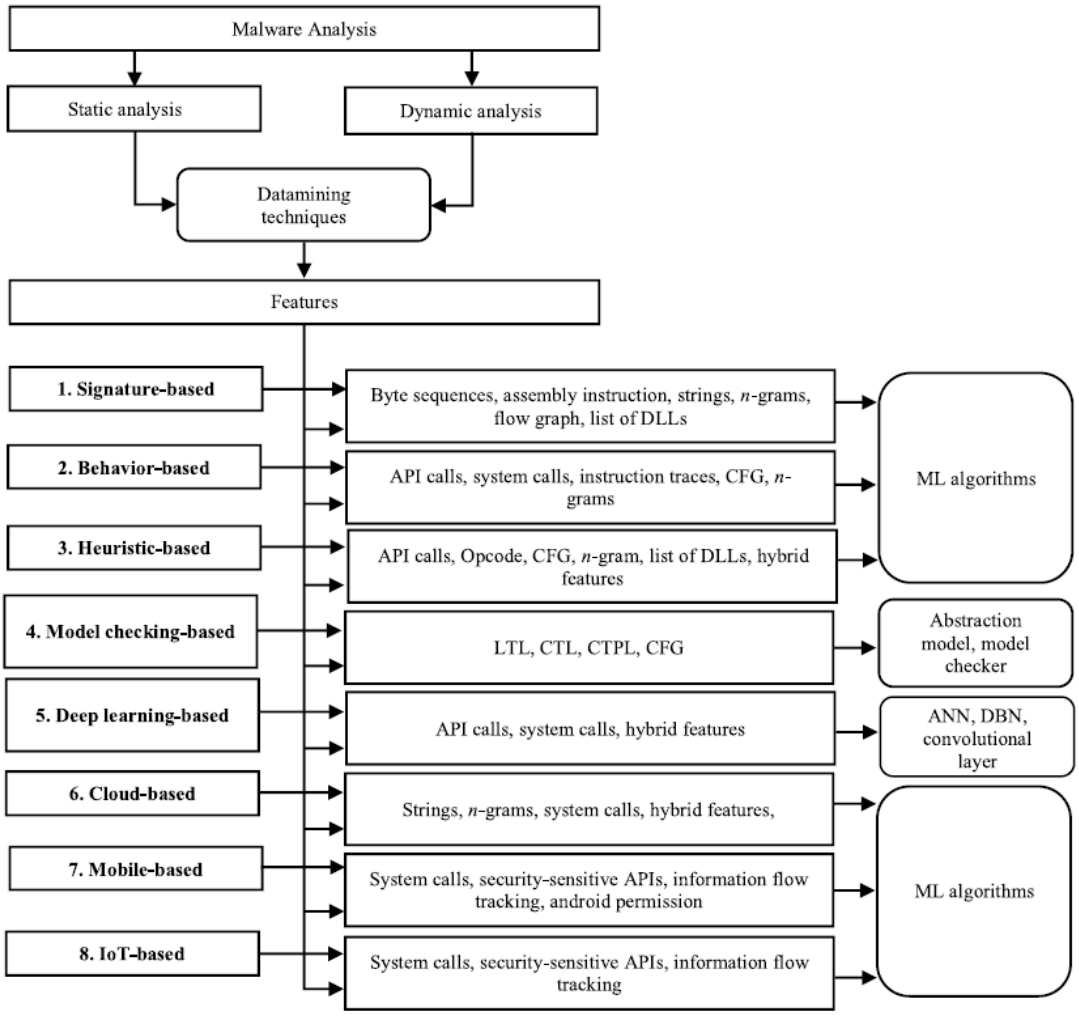

Figure 1: malware detection approaches and features. (OMER ASLAN , AND REFIK SAMET, "A Comprehensive Review on Malware Detection Approaches" , 2019)

Signature-based malware detection:

It's a method that incorporates system configuration and separately identifies malware for each computer. For malware that is already known, the basic signature method works fast and effectively. but it's not sufficient to detect unknown malware. By using obfuscation techniques, a malware program of the same family can easily escape signature-based detection.

In related work for signature based detection, in the paper [39] the researchers work on detecting unknown metamorphic malware. They use the features of n-gram byte string and opcode frequency to get the expected results. Then in [40] the researchers classified PE metamorphic malware by using their proposed method. They use PE anlyze and opcode histogram to do the research work. In the paper[32] researchers go through the detection of meta morphic malware in host base IDS and in network. They use N-gram feature and ML classifier to get the results. Then in [38] researchers introduced a new technique that generates metamorphic virus. They expanding the PE executables and injected the RSA base code functions to achieve the expected result. In paper [36] researchers used PE and insertion of histogram to extract a virus code from a executable that is already infected.

Signature generation process

During the production of the signature, features are first stripped from the executables. The signature creation engine then creates and stores signatures in the signature database. If a sample program has to be classified as harmful or harmless, the relevant sample signature is generated in the same way as previously and compared to the database signatures. The sample software is classified as malware or benign based on the comparison. Entry points, integrity checks, string scanning, and top and tail scanning are just a few of the methods for creating a signature.

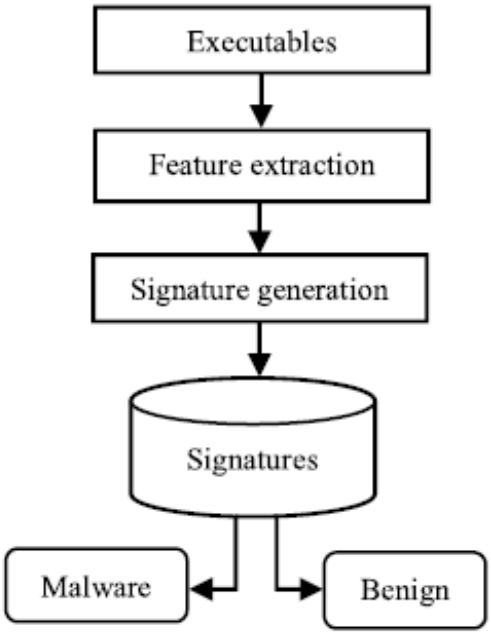

Figure 2: Signature-based malware detection schema.(OMER ASLAN , AND REFIK SAMET, "A

Comprehensive Review on Malware Detection Approaches" , 2019)

Behavior-based malware detection

It detects the behavior of the system with the help of monitoring tools and ultimately, decides(categorize) whether the system is malicious. Program behavior will be the same, although program codes are changed. Therefore, most of the new malicious computer programs can be detected using this approach.

In related work on behavior base detection, in the paper [18] the researchers work on developed a unique method , they named it 'Malhunter' to detect polymorphic malware. The unique method is based on sequence alignment and sequence clustering.

Behavior detection process

First, behaviour is identified using one of the following strategies: automated analysis utilising the sandbox, monitoring system calls, monitoring file changes, comparing registry snapshots, monitoring network activities, and process monitoring in a behavioral-based method.

And data mining is used to extract characteristics from the database.

The categorization is then done using machine learning techniques and specific characteristics from the database.

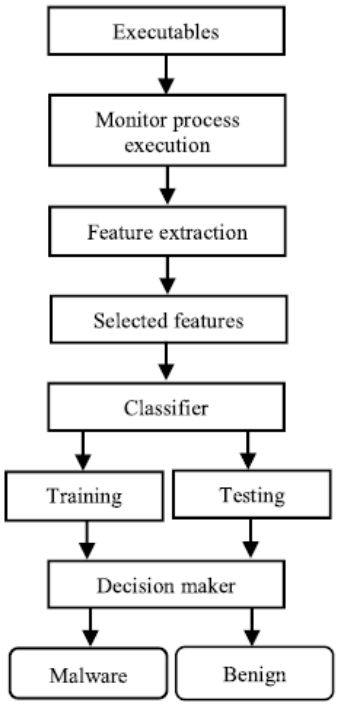

Figure 3: Behavior-based malware detection schema.(OMER ASLAN , AND REFIK SAMET, "A Comprehensive Review on Malware Detection Approaches" , 2019

Heuristic-based malware detection

This approach is a complex technique of discovery that uses different knowledge and method such as the rules and methods of Machine Learning. Heuristic-based detection has good accuracy in detecting malware, but it is not able to detect complex

computer malware.

In related work for heuristic base detection, in the paper [31] researches work on generating PE header heuristic. They use Chi-square test and greedy hill climbing search on PE-header fields to generate the result which is use for detecting meta morphic malware. Then in [35] researcher proposed a HMM base approach that can detect metamorphic malware. They divide a particular part of malware program file and train HMM Aimed file extraction to get the results.

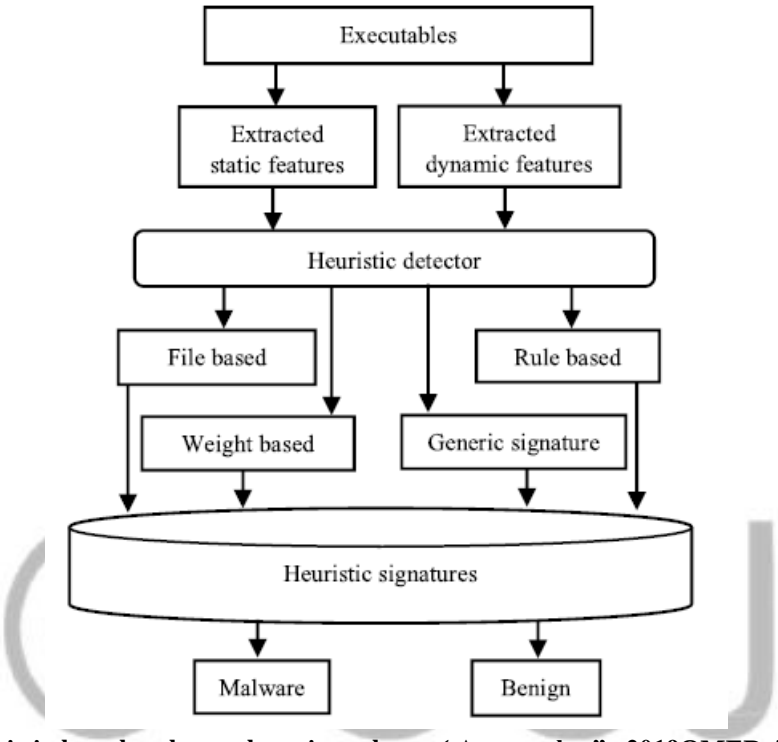

Figure 4: Heuristic-based malware detection schema.(Approaches" , 2019OMER ASLAN , AND REFIK SAMET, "A Comprehensive Review on Malware Detection

Deep learning based malware detection

This acquisition is new and is a widely used method in processing images, unmanned vehicles, voice-control, etc. But cannot be used enough to find a malware program. Deep learning-based work well and reduce feature space significantly, but are not resistant to escape attacks.

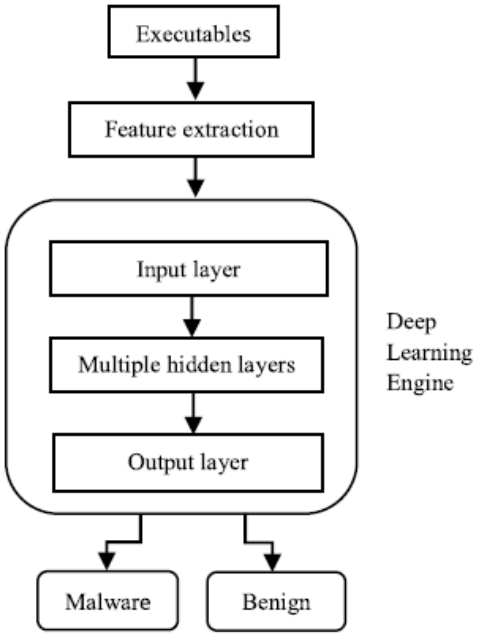

Figure 5: Deep learning-based malware detection schema. (OMER ASLAN , AND REFIK SAMET, "A Comprehensive Review on Malware Detection Approaches" , 2019)

Cloud based malware detection

Cloud computing has grown quickly in recent years due to its several advantages, including simple access, application storage, and cost savings. The cloud must utilise its thunder to identify malware because it contains so much of it. With a large database of malicious software or malware and in-depth computational resources, cloud-based computer optimization has improved the performance of acquisitions for PCs and mobile devices. It helps in providing SAS by using a variety of visual agents over cloud servers.

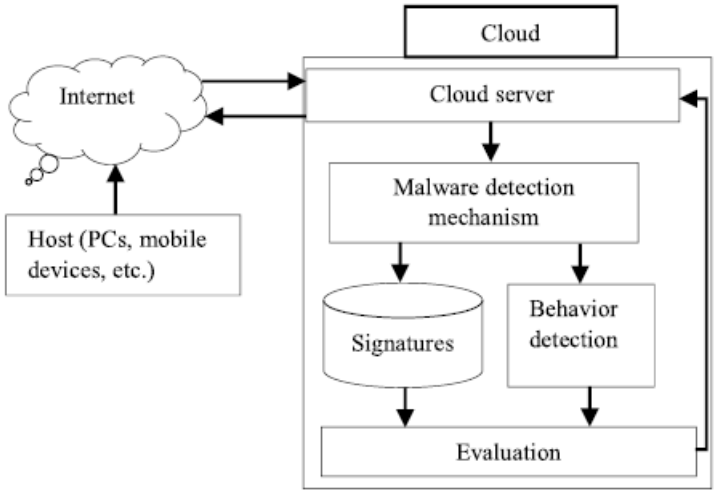

Figure 6: Cloud-based malware detection schema.(OMER ASLAN , AND REFIK SAMET, "A Comprehensive Review on Malware Detection Approaches" , 2019

Evolutionary Algorithm

It is a subset of evolutionary computation. It is a generic population-based metaheuristic optimization algorithm. Evolution algorithm uses biology-evolution inspired methods, such as reproduction, genetic modification, reunification, and selection. Evolutionary algorithms often make solutions for almost all kinds of problems. Strategies from evolutionary algorithms used in the development of evolutionary biological models are generally limited to testing microevolutionary processes.

In related work in the evolutionary algorithm, in the paper [30] the researchers suggest a novel fitness function and a co-evolutionary technique that is a comparison of network dependency to categorized meta morphic malware. Then in [27] researchers work on producing a Zmist malware i.e., a complex variable of malware by using some memetic algorithm. They used HMM clustering and machine learning technique to get the expected result. In the paper [16] researchers proposed a framework that can be used to detect meta morphic malware. They used Machine learning and data source and mutation engine to establish the framework.

Genetic algorithm

It is a metaheuristic-driven natural selection mechanism that makes up a significant portion of evolutionary algorithms.

Biologically inspired operators like as mutation, crossover, and selection are frequently utilised in genetic algorithms to generate high-quality solutions for development and search issues.

In related work on genetic algorithm, in the paper [12] researchers use genetic algorithms to track the evolution of unusual malware. The use of API calls and data mining to get the results through crossover and mutation process.

Hidden Markov model

HMM is one of the most used themes in computational biology i.e., statistical model. It is used to make probability models for labeling problems like linear sequences. HMM provides a conceptual toolset for constructing just by imagining something.

Gene discovery, profile checks, multiple sequence alignment, and regulatory site recognition are all included. Hidden Markov models are the building plans of computational sequence analysis.

API call

API is generally used by every program to send a request to the operating system. The API call sequence is an attractive way of displaying a code piece behavior like malware. Normal behavioral profiles are created using short-track system calls.

Its(API) Call-graph displays the release of a program-related API call sequence made into an executable. A node is represented by a call based on the API used to perform a specific task. The call graph captures API calls in the output file so that API calls may be converted to API Call-grams.

API frequency a is the number of such nodes in the system diagram of the program. The node satisfies two conditions: i) The node has no input margins. ii) The node is

accessible directly or indirectly to an API-compliant location.

Control flow graph

It is a graph that represents flow control systems. It's widely used in software analysis. A target graph with each node representing a system statement and each edge representing a control flow between statements is known as a control flow graph. Assignments, copying statements, branching, and other statements are examples of statements.

A call graph is a control flow graph, representing the calling relationship between two subroutines of a computer system. Each node of the call graph represents a process and each edge indicates a process calling another process.

PE analysis

The PE analysis is mainly used by Windows OS. It is used in malware detection as PE header carries the information of program that ave to rub into the certain portion in memory, address of execution, and binary information.

Greedy hill-climbing search:

It's basically an AI-based algorithm to solve mathematical problems where we consider a graphical chart having y- & and x-axis if x-axis refers to objective function/cost function then y-axis would be state space and our goal is to find the global maximum and local minimum, if cost is optimized then it is called as the greedy approach.

Summary of related works on malware detection approaches and techniques:

Name of paper	Author name	Features representation/ Represent method	Methodology	Accuracy rate	Publishing year
Signature-based Malware detection Approach					
Framework for detecting metamorphic malware-based opcode feature extraction [39]	Prapulla SB, Sharath j Bhat, Shobha G	n-gram byte string, Opcode frequency.	Detecting unknown metamorphic malware using machine learning techniques.	The method gives 96% accuracy rate.	2017

Opcode Histogram for classifying metamorphic portable executable malware [40]	Babak Bashari Rad, Maslin Masrom, Suahimi Ibrahim	PE Analyze, Opcodes Histogram	Classification of metamorphic PE-malware using the proposed techniques.	It has 100% accuracy rate.	2012
Metamorphic malware detection based on support vector machine classification of malware sub-signature [32]	Ban Mohammed Khammas, Alireza Monemi,Ismani Ismall ,Sulaiman mohd Nor and M.N.Marsono	N-gram Feature, ML classifier	detection of metamorphic malware in host-based IDS and network.	The proposed method has a ~99% accuracy rate.	2016
Non-normalizable function : A new metod to generate metamorphic malware[38]	Rodney Owens ,Weichao Wang	Expanding PE Executables, Injection of RSA based code manipulation functions	To introduce a new technique that can generate metamorphic virus, that is done by embedding complicated functions.	The technique used in the paper has an error rate of 0.0014% which means it is 99.9% accurate.	2011
Metamorphic malware detection using based malware identification approach[36]	Devendra Kumar Mahawer and A.Nagaraju	Portable executable, obfuscation and normalization, Histogram intersection.	To extract the virus code from the infected executable	The proposed method has 99.58% accuracy rate.	2013
Behavior-base Malware detection approach					
MalHunter :Automatic generation of multiple behavioral signature for polymorphic malware detection[18]	Haniye Razeghi Borojerdi and Mahdi Abadi	Sequence-based clustering, sequence alignment	To developed a unique method (i.e. Malhunter) that is based on sequence alignment and sequence clustering.	It has 90.83% accuracy rate.	2013

Heuristic-based malware detection					
Using chi-square test and heuristic search for detecting metamorphic malware[31]	Mohamed Belaoued ,Smaine Mazouzi ,Seddari Noureddine and Bouguerou a salah	PE-Header fields, Chi-Square test, Greedy Hill-Climbing Search	To generated PE header heuristics.	The method achieved a 97% accuracy rate.	2015
Proposing an HMM-based approach to detect metamorphic malware[35]	Mina Gharache h ,Vali Derhami, Sattar Hashemi, Seyed Medhi Hazzarati Fard	HMM	Divide the value of a particular part of malware program files to train HMMs aimed file extraction.	It is 92% accurate.	2015
Evolutionary Algorithm					
Metamorphic malware categorization using Co-Evolutionary Algorithm [30]	Zahra Bazrafish an, Ali Hamzeh	Semantic Code, Dependency Graph, co-evolutionary algorithm	To suggested a novel fitness function and a co-evolutionary dependency network comparison technique	N/A The accuracy has not given directly on the paper.	2015
An Intelligent Hunting profile for evolvable metamorphic malware[27]	A.A Ojugo ,A.O.Ebok a	HMM clustering, machine learning	To produce a complex variable of the Zmist malware by the use of a memetic algorithm.	It has a 60.9% accuracy in classificatio n but it has 56% accuracy in detection.	2015
Nowhere metamorphic malware can hide -A biological evolution inspired detection scheme[16]	Kehinde O. Babaagba ,Zhiyuan Tan and Emma Har	data source, disassembly tool, mutation engine, APK, malware detector, ML.	To Propose a framework that can be used in the detection of malware.	N/A.	2018

Compression based detection techniques					
A compression - based technique to classify metamorphic malware[33]	Duaa Ekhtoom, Mahmoud Ali-Ayyoub,Mohammed Al-Saleh Mohammad Alsmirat and Ismail Hmeidi	Approximate Minimum Description Length (AMDL) and Best-Compression Neighbour (BCN)	Determining the origin of a new metamorphic malware.	It has an accuracy of only 11% in AMDL and 67% in BCN.	2016
Static analysis					
Metamorphic malware detection by PE analysis with the longest common sequence[19]	Thanh Naguyen Vu,Toan Tan Nguyen ,Hieu Phan Trung ,Thao Do Duy,Ke Hoang Van, and Tuan Dinh Le	.EXE (PE file), data mining, DLL import, API call.	Determines whether a new executable is metamorphic or benign	It achieved 87.1% accuracy for benign and 92.6% for malware.	2017
Metamorphic malware detection using linear discriminant analysis and graph similarity[37]	Reza Mirzazadeh, Mohammad Hossein Mottar,Majid Vafaei Jahan	Linear Discriminant Analysis ,Opcode Graph Similarity	To detect a malware using the method based on opcode graph similarity.	It achieved 100% and 99% total accuracy for NGVCK and MWOR malware respectively.	2015
Metamorphic Malware Detection Using stastical analysis[29]	Kevadia Kaushal ,Prashant Swadas,Nilesh Prajapati	API calls sequence and frequency,	To use statistical analysis to extract API calls and calculate API frequency to generate feature set.	N/A	2012
Hunting for	Mangesh	Singular value	To detect	N/A	2014

metamorphic javascript malware [15]	Musale ,Thomas H.Austin, Mark stamp	decomposition, Hidden Markov models, Opcode graph similarity, Simple substitution distance	metamorphic JavaScript malware using the proposed method.		
Dynamic Analysis					
A simple Method for detection of metamorphic malware using dynamic analysis and text mining [28]	S.P Choudhary ,Miss Deepti Vidyarthi	Portable executable (PE), DDL, Text mining	To specify how a dynamic report can be analyzed and how to prepare the model That can help in taking decisions on detection.	It classifies malware with a 97.8% accuracy rate.	2015
Enhancing the detection of metamorphic malware using call graphs [34]	Ammar Ahmed E.Elhadi ,Mohd Aizaini Maarof ,Bazara I.A Barry , Hentabli Hamza	graph matching algorithm,API call graph	To convert random malware samples into an API call graph with the operating system resource (that represents graph nodes) and integrates API calls.	This system gets success with 98% accuracy.	2014
Metamorphic Malware Detection Using Function Call Graphs Analysis [11]	Prasad Deshpande ,Mark Stamp	Function call graph, Hidden Markov model (HMM), Opcode analysis.	To implemented the function call graph method and applied to the malware detection problem.	N/A	2016
Genetic algorithm					
A novel method for detecting future generation of targeted and metamorphic malware based on genetic algorithm [12]	Danial Javaheri, POOIA LALBAKSH, and Mehdi Hosseinzadeh	API calls, Metamorphism, Data mining,	To use genetic algorithms to track the evolution of unusual malware through crossover and mutation processes	It is 96% accurate.	2017

Conclusion

Since 2018, worldwide malware attacks have risen by 350% in total. There has been a lot of development in malware detection approaches over the years. But none of them has been able to fully or successfully able to detect the malware. The detection for newly generated ones becomes harder due to their sophistication. Like in the case of Machine Learning and signature base technique the model provides a strong methodology in feature selection. The system gives better results if the machine is fed with more datasets and trained. This shows that although having such a success rate of detection, there remains some or the other liability. The signature-based approach is one of the fast and most effective methods for known viruses but is unable to detect unknown ones. Deep learning-based detection is highly successful, and it also dramatically decreases feature space, but it is vulnerable to evasion attempts. The heuristic-based malware detection technique has also a good success rate, for eg: Using the chi-square test and heuristic search for detecting metamorphic malware[31], stated that this technique has a success rate of 97% in generating PE header heuristic. But it also has some shortcomes, like it cannot detect complex malware. And, likewise, we have discussed a lot of techniques and methods that are being used nowadays. And most of them have excellent rates of success.

Recently the severity of metamorphic attacks has become common. Due to this lots of companies are going on safety first approaches. They are hiring a lot of talents to tackle the attacks beforehand. As it is better to detect the problem before it can inflict damage to the system. This review paper aimed to give you an idea about the up-thrusting problems of metamorphic malware. The dangers it poses to our system and our data (personal information). We have presented a detailed review of the techniques and algorithms that are being used till now to detect and analyze metamorphic malware. The advantages and disadvantages are also being discussed.

REFERENCES

[1] Steven Strandlund Hansen, Thor Mark Tampus Larsen, Matija Steavanovic, Jens Myrup Pedersen, ”An approach for detection and family classification of malware based on behavioral analysis” 2016 International Conference on Computing, Networking and Communications (ICNC), Workshop on Computing Networking and Communication.

[2]Gerald R. Thompso n and Lori A. Flynn, “Polymorphic Malware Detection and Identification via Context-Free Grammar Homomorphism “ Bell Labs Technical journal 12(3),139-147(2007)© 2007 Alcatel -Lucent.Published by wiley periodicals,inc.Published online in Wiley InterScience (www.interscience.wiley.com)

[3]Amit Sahu ,Prachi Parwar ,Deepak Agrawal ,”An Analysis to Detect Malware using Machine Learning” IJSART-Volume 5 Issue 9 -SEPTEMBER 2019

[4]Abhijit Yewale, Manindar Singh, " Malware Detection Based on Opcode Frequency" 2016 International Conference on Advanced Communication Control and Computing Technology (ICACCCT)

[5]Vijay Naidu, Ajit Narayan "Further Experiments in Biocomputational Structural Analysis of Malware " 2014 10th International conference on natural computation

[6]Silvio Cesare and Yang Xiang "A Fast Flowgraph Based Classification System for packed and polymorphic malware on the end host" 2010 24th IEEE International Conference on Advanced Information Networking and Applications.

[7]Zahra Bazrafshan, Hashem Hashemi, Seyed Mehedi Hazrati Fard , Ali Hamzeh "A Survey on Heuristic Malware Detection Techniques" 2013 5th conference on information and knowledge technology (IKT)

[8]Jake Drew ,Tyler Moore, Michael Hasher "Polymorphic Malware Detection Using Sequence classification methods" 2016 IEEE Security and Privacy workshop.

[9]Joma Alrzini ,Diane Pennington "A review of polymorphic malware detection techniques"

[10]Vinayak Kumar , Mamoun Alazab ,Soman KP , Prabaharan Poornachandran and Sitalakshmi Venkatraman "Robust Intelligent Malware Detection Using Deep Learning"

The article has been accepted for publication in a future issue of this journal but has not been fully edited

[11]Prasad Deshpande ,Mark Stamp "Metamorphic Malware Detection Using Function Call Graphs Analysis" MIS Review Vol 21 ,Nos ½ ,September (2015)/March(2016),pp 15-34 DOI:10.613/MISR.2015.2101.02

[12]Danial Javaheri(Member ,IEEE),POOIA LALBAKSH, and Mehdi Hosseinzadeh "A novel method for detecting future generation of targeted and metamorphic malware based on genetic algorithm"

[13]Oinghua Zhang ,Douglas S.Reeves

"Metaware :Identifying Metamorphic Malware "

This work supported by by the national science foundation (NSF)under grant CNS -0627505

[14]Li Wang , Dongpeng Xu ,Jiang Ming "MetaHunt :Towards Taming Malware Mutation via Studying the Evolution of Metamorphic virus".

[15]Mangesh Musale ,Thomas H.Austin,Mark stamp "Hunting for metamorphic javascript malware " J Comput Virol Hack Tech DOI 10.1007/s11416-014-0225-8

[16]Kehinde O. Babaagba,Zhiyuan Tan and Emma Hart "Nowhere metamorphic malware can hide -A biological evolution inspired detection scheme.

[17]Yanzhen Qu,Kelly Hughes "Detecting metamorphic malware by using behaviour -based agrgregated signature " World congress on internet security (worldCIS-2013)

[18]Haniye Razeghi Borojerdi and Mahdi Abadi "MalHunter :Automatic generation of multiple behavioral signature for polymorphic malware detection" 3rd international conference on computer and knowledge engineering(ICCKE2013),October 31 & November 1,2013 ,Ferdows university of Mashhad

[19] Thanh Naguyen Vu,Toan Tan Nguyen ,Hieu Phan Trung ,Thao Do Duy,Ke Hoang Van, and Tuan Dinh Le "Metamorphic malware detection by PE analysis with the longest common sequence"

[20] Yahonatan Cohen ,Danny Hendler "Scalable Detection of Server-Side Polymorphic Malware "

[21]Vijay Naidu ,Ajit Narayanan " A Syntactic Approach for detecting viral polymorphic malware variants"

[22] Natahan Pors "The effective of self -mutating malware detection techniques."

[23]Nur Syuhada Selamat,Fakariah Hani Mohd Ali ,Shah Alam ,Noor Ashitah Abu Othman "Polymorphic Malware Detection"

[24]Kirti Mathur, Saroj Hiranwal " A survey on techniques in detection and Analyzing Malware Executables " International Journal of Advanced Research in computer science and softwere engineering"

[25] Emmanuel Masabo,Kyanda Swaib Kaawaase, Julianne Sansa-Otim, Damien Hanyurwimfura "Structural Feature Engineering approach for detecting Polymorphic malware " 2017 IEEE 15th IntL Conf on Dependable ,Autonomic and secure computing ,15th Intl Conf on pervasive intelligence and computing ,3rd on big data intelligence and computing cyber science and technology Congress"

[26]Andrew Walestein ,Rachit Mathur ,Mohamad R . Chouchane and Arun Lakotia

" The Design Space of Metamorphic Malware "

[27] A.A Ojugo ,A.O.Eboka "An Intelligent Hunting profile for evolvable metamorphic malware " African journal of computing & ICT.

[28] S.P Choudhary ,Miss Deepti Vidyarthi "A simple Method for detection of metamorphic malware using dynamic analysis and text mining" Eleventh International Multi-Conference on information processing-2015 (IMCIP-2015).

[29]Kevadia Kaushal ,Prashant Swadas,Nilesh Prajapati " Metamorphic Malware Detection Using stastical analysis " International journal of soft computing and engineering

[30] Zahra Bazrafishan ,Ali Hamzeh "Metamorphic malware categorization using Co-Evolutionary Algorithm " IKT2015 7th international conference on information and knowledge technology.

[31]Mohamed Belaoued ,Smaine Mazouzi ,Seddari Noureddine and Bougueroua salah "Using chi-square test and heuristic search for detecting metamorphic malware "

[32]Ban Mohammed Khammas ,Alireza Monemi,Ismani Ismall ,Sulaiman mohd Nor and M.N.Marsono "Metamorphic malware detection based on support vector machine classification of malware sub-signature" TELEKOMNIKA vol.14 No.3 september 2016 .pp 1157~ 1165

[33]Duaa Ekhtoom, Mahmoud Ali-Ayyoub,Mohammed Al-Saleh Mohammad Alsmirat and Ismail Hmeidi "A compression -based technique to classify metamorphic malware " .

[34] Ammar Ahmed E.Elhadi ,Mohd Aizaini Maarof ,Bazara I.A Barry , Hentabli Hamza "Enhancing the detection of metamorphic malware using call graphs" Computer & security 46(2014)62-78

[35] Mina Gharacheh ,Vali Derhami ,Sattar Hashemi , Seyed Medhi Hazzarati Fard "Proposing an HMM-based approach to detect metamorphic malware " 2015 4th Iranian Joint congress on fuzzy and intelligent system (CFIS)

[36] Devendra Kumar Mahawer and A.Nagaraju "Metamorphic malware detection using based malware identification approach " Security and communication network published online 6 november 2013 in wiley online library (wileyonlinelibrary.com)

[37] Reza Mirzazadeh, Mohammad Hossein Mottar,Majid Vafaei Jahan "Metamorphic malware detection using linear discriminant analysis and graph similarity" 2015 5th International Conference on computer and knowledge engineering(ICCKE).

[38]Rodney Owens ,Weichao Wang "Non -normalizable function : A new metod to generate metamorphic malware " The 2011 Military communication conference -Track3-Cyber security and network operation.

[39] Prapulla SB ,Sharath j Bhat,Shobha G "Framework for detecting metamorphic malware based opcode feature extraction " 2nd IEEE international conference on computational system and information technology for sustainable solution 2017.

[40] Babak Bashari Rad ,Maslin Masrom ,Suahimi Ibrahim "Opcode Histogram for classifying metamorphic portable executable malware"