Inclination of Computer Virus and Anti-Virus Techniques A Short Survey

Ali Aziz[1], . Ans Bin Jawaid[2],Hassan Raza Khan[2]

Abstract— In today's world computer viruses are a big problem for everyone who uses computer. This survey report presents the general view about the development of computer viruses and defense mechanisms of anti-viruses to stop them. In order to prevent from the detector of anti-viruses, computer viruses regularly upgrading their codes. Anti- viruses programs uses several distinctive methods in inspecting, scanning, detecting malwares to deliver enough shelter for computer systems .We also presents a comparison table which shows the strengths and weaknesses of every detection methods and also evaluate their features. In the end we also give some future recommendations .and conclusions

Keywords— Encryption, Virus, Anti-virus, trend, defense .mechanism, generations

INTRODUCTION

Since the beginning of malware creations, it has been an enormous challenge between the programmers who code the viruses and the antivirus specialists. Due to this rivalry between them there has been vast list of malware programs and viruses introduced almost every day and also the protection system which prevents or eliminate them have been developing in accordance. Virus is a program that copies its code into other non-infected programs and infects them when executed [1].

We can define a "Computer Virus" as a program or coded script which can enter in our private system and modify them, making a complete identical copy or similar which will allow it to be hidden for a specific period of time [2]. A virus makes unwanted changes in the program which might result in complete deletion of our required data or partial loss. The number of new viruses are increasing over the last years and increasing in growth [3].

First we are going to describe the evolution of viruses, with classification and description of viruses then we will move towards the methodologies used by anti-virus systems to protect the computers and other database systems from these viruses and malware programs. The most important thing for virus makers is to make the virus life long as possible [4] The anti-virus programs uses distinct approaches of examine, scanning and detecting the malwares which allows them to ensure security to the computer systems from

new viruses to enter and also elimination of currently present viruses in system. Anti-virus software's are used for the detection and for the removal of viruses from computer, also try to diminish the impact of viruses on any data [5]. We will also have a look at the comparison table, which will allow us to compare the advantages and disadvantages of methodologies used by anti-virus. Then we will move towards the conclusion and give some recommendations regarding the topic. A virus infects other computer systems through any software, for internet users the virus often comes from downloading files via FTP (File Transfer Protocol) [6].

David Gerrold was the first person to use term "virus". A computer virus is an unwanted segment of machine code (typically from 200 to 4000 bytes) which will make copies of itself or modified self when it is active. If the program which has already been infected by the virus will be executed then the virus will further spread into the system and make its roots stronger. The program that become infected by virus also represent a virus that is how infection spreads [7].

Research Trend

The papers published on development of computer viruses and anti-viruses techniques are shown in below since January 2011 to September 2021 are in Fig.1 given below:

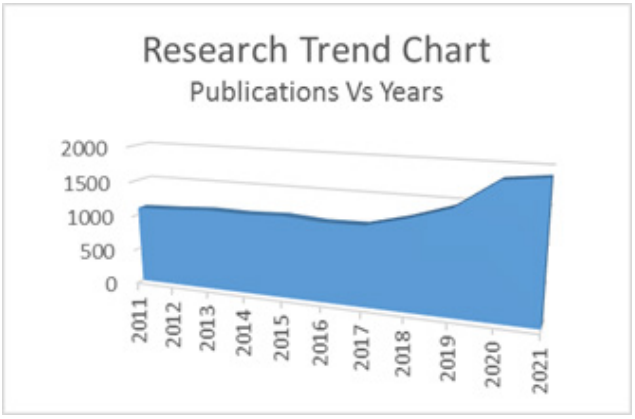

Fig.1. Number of publications since 2011

[1]Shanghai Jiaotong University Shanghai, China
[2] Iqra University Karachi, Pakistan
Email: * aliaziz786@sjtu.edu.cn

From the above graph, it is found that a great number of and increased rapidly from the year 2011 to the year 2021. But in the year of 2014 the number of published papers is in very small quantity

TYPES OF VIRUSES

Encrypted Viruses

Encryption is the very simplest way to shield the virus codes [8]. Encrypted virus is the combination of two key parts: a decryption code, and a virus which is encrypted [9]. Encryption is the method of converting data which travels through networks into a code and the key is provided to authorized person who as a decryptor uses that code to decipher the data from encryption. In encrypted virus the body of a virus is encrypted with different encryption algorithms and each algorithm requires a different decryptor as well [10]. Encryption is also applied to make viruses more hidden and hard to detect [11]. The encryption of a virus was first done in 1988. Encrypted virus is integration of two key components, the encrypted body and a tiny decryption code which can decrypt the virus when detected. Encryption works as a two layered barrier which keeps the virus code hidden from the viewers and as well as moderate the infected files.

Metamorphic Viruses

Metamorphic Viruses are able to reprogram automatically by using a technique called obfuscation technique to make the children don't look like parent [12]. Metamorphic viruses changes it appearance, code from infection to infection. Antivirus Specialists spend a long time to make a new polymorphic virus which might not spread out broadly, but they manage the detection of such viruses in a moment [13]. "Metamorphic virus is a body polymorphic virus" is the shortest definition of metamorphic virus quoted in [14] by Peter Szor defined by Igor Muttik. Metamorphic viruses can modified automatically using some obfuscation techniques. A well-known example of fully metamorphic virus is Lexotan32, none of the antivirus scanners able to detect all the samples of this metamorphic virus [15]. Metamorphic viruses evade the detection from anti-virus software as each variant will have different signature. They use the idea of polymorphism. Polymorphic virus encrypt the virus and change the decryptor, whereas metamorphic viruses change the whole virus code, to conceal it from any possible signature, therefore there is no need to encrypt the virus code [16]. Hidden Markov Models (H.M.Ms) are very helpful in the detection of metamorphic viruses [17].

Oligomorphic Viruses

Anti-virus software's very easily detect encrypted viruses so that virus makers realize this and to challenge anti-virus products they implement a system to generate transmute decryption [18]. Semi polymorphic viruses is another name of oligomorphic viruses [19]. Virus makers are trying to create those encryption methods that cover up the viruses of first generation. But the decryptor loops were remain unchanged in newly infected files. Which means that the anti-

virus software are able to scan or detect such viruses for which signature string was easily achieved [20]. To incapacitate this susceptibility, the virus makers trying different methods to made a modified body for decryptors [21]. As a result of these efforts a new kind of virus obtained named as oligomorphic virus.

Polymorphic Viruses

The highly common technique used in anti-viruses software to find out the viruses is signature scanning [22]. Polymorphic viruses are capable of changing its appearances in hope to avoid the detection from antivirus software. Polymorphic viruses are pretty much tough to employ and handle [23]. Polymorphic viruses changes its form regularly, it makes detection process more difficult. Its change of form or appearance of code is its principal rule [24]. Polymorphic viruses modify itself although keeping the primary code in one place. Polymorphic virus uses metamorphic decryptors for avoiding the detection from antivirus. A polymorphic virus is the most complicated type of encryption and oligomorphism. It is similar to encrypted and oligomorphic viruses in encryption of code, but polymorphic viruses creates unlimited new copies of decryptors [25]. Polymorphic virus is similar to encrypted virus. It uses the concept of encryption, and one step further of encrypted virus [26]. To evade the detection from anti-virus so polymorphic viruses use metamorphic decryptors. Polymorphic malwares, oligomorphic malwares and encrypted malwares all are same, but the difference is that polymorphic malware has the potential to generate limitless new copies [27].

LITERATURE REVIEW

In this section we will briefly discussed about the generations era of detecting techniques as we can also find in Fig. 2.

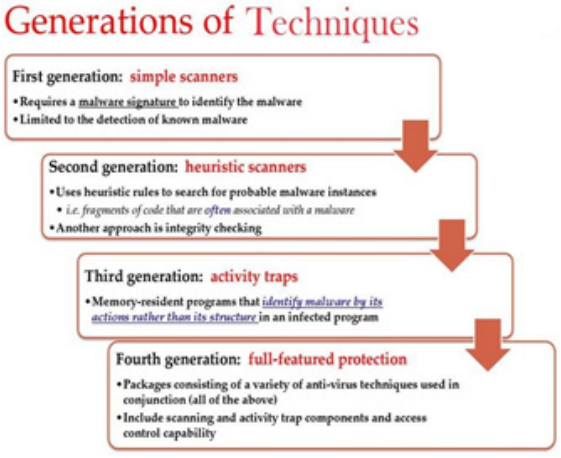

Fig.2. Generations of virus & anti-virus techniques.

First-Generation Scanners

Detection of computer viruses developed since cohen first computer virus reinforced in 1983 [28]. First generation scanners don't uses complex methods to uncover the computer virus. Initial scanners are only watched for sequence of bytes known as string scanning. For this anti- viruses scans binary pattern of files to discover the strings, if it finds recognized sample, it alert for the recognition of malware. A string consists of 16 bytes. . It is the most common method used by anti-virus scanners. These scanners work well only for known viruses [29]. First generation scanners uses the signature to discover the viruses. It hunts for the signature of viruses.

Defense mechanisms of first generation scanner

Every detection method have some problems, most of the detection techniques is not good for the detection of new viruses also it is difficult to detect those viruses or malwares that behaves normally [30]. The mechanism used for first generation scanners is based on string scanning with different methods.

Special Cases in String Scanning

There are three useful cases in string scanning.

(i)Wildcards:

Wildcards are used to prevent some byte values from evaluation for Example, in the given string, bytes are determined by "?". The "%2" point out the scanner to locate the byte value in two upcoming places.

9A45 01?? C003 E76C%2 FF7C A4B7 B401 D578

Use of wildcards allows anti-virus scanners to skip some characters from the target string, it increases the speed of algorithm [31]. Some encrypted and polymorphic viruses can be detectable by wildcard [32].

(ii)Mismatch:

Mismatch permits small values for the number of bytes in a string, irrespective of their rank. This method is introduced by IBM antivirus, it allows finite number of bytes in the string [33].

(iii)Generic Degree:

There are four steps or emulators of a generic detection processor, memory, system, and decision mechanism [34]. If the malware has additional variant, the variants are scanned to take out one string that represent all of them. The kind of string scanning uses some sample to locate a virus. It also uses wildcards and mismatches to shelter the samples of the viruses. It is basically related to the different versions of viruses or the different forms of a virus. The generic degree helps to reduce the different versions of a viruses by identify a mutual signature which is common to all the viruses. This decreases the number of search strings.

Bookmarks

Bookmark is the simplest way to make sure a more consistent detection and there is no danger of false detection. For example, for the boot virus bookmarks show the address of boot sectors, also the size of the viruses is very beneficial bookmark [35].

Speed-up Techniques

As nearly all scanning techniques taking much time to match the input statistics with the earlier recognize worm signature, so it is necessary to design the algorithms to overcome this problem and making the scanning process faster. Two of the most common techniques are given below.

(i)Hashing:

It is the most common method used for searching purpose. Hashing makes searching data access faster [36]. It decreases the number of searching strings in file by using 1 byte or 16 bit word of the scanned string for producing the hash function. It also improves the speed of the scanning process.

(ii)Top-and-Tail Scanning:

Top and tail means scanning the first and last part of file only. It is faster than hashing function. This method is introduced by IBM antivirus, it allows finite number of bytes in the string. As the code of the viruses are situated usually in the opening or in the conclude of the file being infected by viral attack. The top and tail scanning function scans only the first and last part of file instead of scanning the whole so it is less time consuming than the previous searching methods, but it is not more reliable than hashing function because it only scans the specific areas.

Second-Generation Scanners

The second-generation scanners starting to build on, when the scanning methods for the detection of new viruses lost their effectiveness. This generation scanners initiated exact recognition which makes anti-viruses more trustable. The second generation scanners work for new viruses [37].

Defense mechanisms of second generation scanner

Its mechanism is based on some scanning pattern

Smart Scanning

Smart scanning is the defensive optimization technique, which try to hide its code within NOP commands. After modification of virus tools starting to build on, signature scanning is not powerful method because these kits construct that are viruses much different from original look. Smart scanning leave out commands like NOP, and does not count

them as the signature of virus. In addition, smart scanning is used for the detection of macro viruses print in text form. Smart scanning improves the quality of detection, by ignoring some characters used to mutate the virus codes, like Space and TAB characters.

Skeleton Detection

It is widely used to detect the micro viruses. This method is introduce by Kaspersky anti-viruses it reduces the search zone in the file [38]. The idea is that before starting of scanning process, first eliminate all instructions that are not part of virus. It takes less time to search because it does not search the entire areas that is not scan the area belongs to code of virus. The code skeleton stayed only with the macro code due to which it is utilize by scanners for virus detection [39]. It only search the areas being infected by virus. It also removes any unimportant statement from the file, and it is faster than smart scanning method.

Exact Identification

It ensures the accurate detection of variants of virus. It also use the combination of first generation scanning techniques. The advantage of exact identification is that it is easily implemented, and disadvantage is it slowing the scanning method

Heuristics Analysis

It is very useful method for detecting the newly updated unknown viruses. It is very helpful in detection of new viruses and the detection of macro viruses too [40-41], but the disadvantage of this scanner is that, it produces false positive output in some cases below is the mechanism of heuristics analysis in Fig. 3.

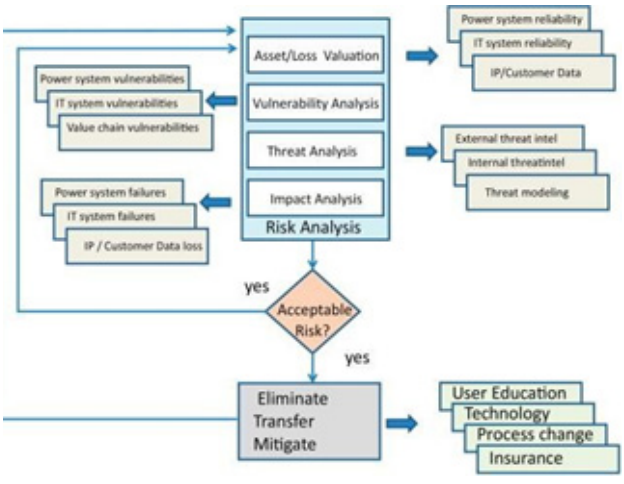

Fig.3. Heuristics analysis flow diagram.

It identify virus by looking for code that performs suspicious functions. Heuristics analysis used two methods.

1.Static Analysis Method
2.Dynamic Analysis method

The static analysis method is use to find the structure of file and the code of virus, and dynamic analysis method uses the code analysis method to distinguish the reaction of program. Heuristics analysis is also helpful in detecting the macro viruses. It also helpful for the detection of binary viruses as well, but it might generates false result that is the disadvantage of this scanners.

Virus-specific Detection

Generally the algorithm made for overall virus detection are not capable to deal with some kind of viruses. A virus specific detection method is to be designed for making the detection procedure more reliable. This method is designed for the specific type of viruses, so it is not a regular method.

Filtering

It is the extension of virus specific detection method. The Virus specific detection methods are very time consuming so filtering method optimized the anti-virus engine performance. The programs like .EXE and .COM only infected by executable viruses, and macro viruses. Infect document that perform macro statements. During specific file searching it checks only relevant material to hold the scanning time miserable.

X-RAY Scanning

X-Ray scanning is the type of virus specific detection, but it is used to detect only the virus which has encrypted code. It attacks encryption of viruses instead of searching the description. X ray scanning takes the advantage of the weaknesses in the encryption algorithm of viruses [42]. Its disadvantage is that it required more time for searching if the beginning of virus is not situated on permanent location.

KEY FINDINGS IN LITERATURE

From literature review it seems that, the anti-viruses creators are making efforts to overcome the viruses. Although virus makers are one move further on, since they pick what way to attack and anti-virus software has to only shield in contrast their attack. First generation scanners only helpful for detection known viruses only, but second generation scanners are very helpful for the detection of new viruses. And also every anti-virus software has some disadvantages and weaknesses that helps virus makers to accomplish their goal

OPEN AREA

There are numerous weaknesses in both the virus and anti-virus technologies, but majorly the anti-virus program lacks in the detection of a virus. The scanning process takes a

substantial expanse of time, whereas prior detection is not strong without the updates being done to the anti-virus program. The virus databases must be more and more advanced to check and balance the current situations of system.

We have also concluded that there is a huge amount of expenditure being spent on the virus and malware anti-virus technologies which is in Thousands of US dollars per Month.

Our recommendation is that the organizations should purchase the licensed software's as the unlicensed one are potentially viable to the viruses and can be easily damaged. Also, the anti-virus program must be installed and be updated as soon as the update arrives in the archive. The prevention methodology should be used against detection because when the virus has already accessed in your system it can damage your files in the time you will spend in detection of the virus.

Organizations should create awareness in their staff to be extremely aware of not using bad sources to download or to browse un-authentic websites. For controlling these activities a proper platform must be provided by creating proper information technology system.

CONCLUSION

In this paper, we have tried our best to cover all the viruses and anti-virus detection techniques but it's also impossible to do so in such a short research survey. We can clearly conclude from our studies that the virus coders or conventionally hackers who develop these viruses are more clever and ahead of the anti-virus coders. As we know that the offensive one is always on an advantage as he seeks just a slight gap to attack and destroy. While the anti-virus which defends through the viruses must be very active to keep check on these attacks and counter them before they cause a major problem. The anti-virus developers must do more and more research to predict the future coming threads before it takes the bait.

REFERENCES

[1] Rohith, Cheerala, and Gagandeep Kaur. "A Comprehensive Study on Malware Detection and Prevention Techniques used by Anti-Virus." 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM). IEEE, 2021.

[2] Jaiswal, Manishaben. "Computer Viruses: Principles of Exertion, Occurrence and Awareness." International Journal of Creative Research Thoughts (IJCRT) (2017): 648-651.

[3] Rad, Babak Bashari, Maslin Masrom, and Suhaimi Ibrahim. "Evolution of computer virus concealment and anti-virus techniques: a short survey." arXiv preprint arXiv: 1104.1070 (2011).

[4] Menéndez, Héctor D., and José Luis Llorente. "Mimicking anti-viruses with machine learning and entropy profiles." Entropy 21.5 (2019): 513.

[5] Babak Bashari Rad, "Camouflage in Malware: from Encryption to Metamorphism", International Journal of Computer Science & Network Security. Aug 2012, Vol. 12 Issue 8, p74-83. 10p.

[6] Sarika Choudhary, Ritika Saroha, Sonal Beniwal, How Anti-virus Software Works? International Journal Of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013 ISSN: 2277128X.

[7] Sandeep Kaur, Analysis of Various Types of Viruses and their Remedies", Lovely Professional University, Phagwara, Dept of Computer Science, Volume 4, Number 1 (2012), pp. 9-18.

[8] Henry Osborn, "The Economic Impact of Computer Virus - A case of Ghana", REGENT UNIVERSITY COLLEGE OF SCIENCE & TECHNOLOGY, ACCRA, GHANA, VOL. 3, NO. 8 August, 2012 ISSN 2079-8407.

[9] Szor, P., the Art of Computer Virus Research and Defense, Addison-Wesley Professional, 2005

[10] Skulason, F., "Virus Encryption Techniques", Virus Bulletin, November 1990.

[11] Konstantinou, Evgenios, and Stefen Wolthusen. "Metamorphic virus: Analysis and detection." Royal Holloway University of London 15 (2008): 15.

[12] Priti Desai and Mark Stamp, "A Highly Metamorphic Virus Generator", Department of Computer Science San Jose State University

[13] Arun Lakhotia, Aditya Kapoor, Eric Uday, "Are Metamorphic Viruses Really Invincible? Part 2", VirusBulletin, January 2005.

[14] Szor, P., "The new 32-bit medusa", Virus Bulletin, December 2000.

[15] Szor, P. and P. Ferrie, "Hunting for Metamorphic", in 11th Virus Bulletin International Conference, 2001.

[16] Virus magazine. http://vx.org.ua/29a/29A 6. Html, Section 29a, page#6, last visit: September. 2021.

[17] Priti Desai and Mark Stamp, "A Highly Metamorphic Virus Generator", Department of Computer Science San Jose State University 2010.

[18] S. Attaluri, S. McGhee, and M. Stamp, Profile hidden Markov models and metamorphic virus detection, Journal in Computer Virology, Vol. 5, No. 2, May 2009.

[19] Ankush R Kakad, "Study and Comparison of Virus Detection Techniques ", Computer Science India,
Volume 4, Issue 3, March 2014

[20] Aycock, J., Computer Viruses and Malware, New York, NY, USA: Springer, 2006.

[21] Babak Bashari Rad, "Evolution of Computer Virus Concealment and Anti-Virus Techniques", International

Journal of Computer Science Issues (IJCSI). Jan 2011, Vol. 8 Issue 1, p113-121. 9, p. 2.

[22] Szor, P., the Art of Computer Virus Research and Defense, Addison-Wesley Professional, 2005.

[23] Zhang, Q., "Polymorphic and metamorphic malware Detection", Ph.D. Thesis, ^Graduate Faculty, North Carolina State University, Raleigh, NC, USA, 2008.

[24] Karim, Md Enamul, et al. "Malware phylogeny generation using permutations of code." Journal in Computer Virology 1.1 (2005): 13-23.

[25] P. O'Kane, S. Sezer, and K. McLaughlin, "Obfuscation: The Hidden Malware," Security & Privacy, IEEE, vol. 9.

[26] S. Noreen, S. Murtaza, M. Z. Shafiq et al., "Evolvable Malware," in Proceedings of the 11th Annual conference on Genetic and evolutionary computation, Montreal, Canada 2009.

[27] Priti Desai and Mark Stamp, "A Highly Metamorphic Virus Generator", Department of Computer Science San Jose State University 2010.

[28] Vinod P." Survey on Malware Detection Methods", Department of Computer Engineering, Malaviya National Institute of Technology, Jaipur, Rajasthan, last visited:
September 2021

[29] F. Cohen. Viruses. PhD. Thesis, University of Southern California 1985.

[30] Bist, Ankur Singh, "Hybrid model for Computer Viruses: an Approach towards Ideal Behavior", International Journal of Computer Applications. May 2012, Vol. 45, p16-19. 4p

[31] E Daoud and I. Jebril, "Computer Virus Strategies and Detection Methods," Int. J. Open Problems Compt.
Math., Vol. 1, No. 2, September 2008

[32] Catalin, B. and A. VI Oiu, "Optimization of Antivirus Software", Informatica, Vol. 11, 2007.

[33] Szor, P. and P. Ferrie, "Hunting for Metamorphic", in 11th Virus Bulletin International Conference, 2001,

[34] Catalin, B. and A. VI Oiu, "Optimization of Antivirus Software", Informatica, Vol. 11, 2007.

[35] Veldman, F., "Generic Decryptors Emulators of the Future", in IVPC conference, 1998.

[36] F. Cohen, "Computer viruses: theory and Experiments" Computer Security, 1987.

[37] Henry Osborn, "The Economic Impact of Computer Virus - A case of Ghana", REGENT UNIVERSITY

COLLEGE OF SCIENCE & TECHNOLOGY, ACCRA, GHANA, VOL. 3, NO. 8 August, 2012 ISSN 2079-8407.

[38] Arnold, W. and G. Tesauro, "Automatically Generated Win32 heuristic virus detection", in 10th Virus Bulletin International Conference (VB2000), 2000.

[39] S. Attaluri, S. McGhee, and M. Stamp, Profile hidden Markov models and metamorphic virus detection, Journal in Computer Virology, Vol. 5, No. 2, May 2009.

[40] Virus Bulletin International Conference, 2001.

[41] Chavan, Akshay, Keerti Kerakalamatti, and Snigdha Srivastva. "Implementation of Portable Antivirus System using Signature-based Detection and Heuristic Analysis." 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2021.

[42] Perriot, F. and P. Ferrie, "Principles and practice of x-Raying", in 14th Virus Bulletin International Conference, 2004.