IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 7, July 2022

A Review on Antivirus Pattern

Anu Sharma, Assistant Professor,
College of Computing Sciences and Information Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- er.anusharma18@gmail.com

ABSTRACT: ***Computer viruses are executable code programs that have a unique ability to replicate themselves in computer system and spread rapidly from one computer to another affecting file, documents and programs to alter their normal running. Viruses are represented as patterns of computer instructional codes that exist over time in computer systems. Antiviruses on the other handare programs specially developed to counter challenges brought about by viruses as they protect thecomputer systems from virus attacks by heavily relaying on the controls enhanced in their databases. Antiviruses therefore scan the computer using some specific patterns of bytes indicative of known viruses. To stay current, they must be developers of these antiviruses update their databases whenever new viral strains arise. This paper reviews the various virus and antivirus patters and various detection schemes. Today, safety of our data is a big question from various threats come from online and offline. The user should protect their valuable data from these threats using different antivirus software tools available in market. Before going to install an antivirus software tool, the user should know the performance, features, help and support given by the antivirus software tool providers. This analysis will help in this situation.***

KEYWORDS: Antiviruses, Patterns, Software, Threats, Viruses.

1. INTRODUCTION

Computer viruses [1] are executable code programs [2] that have a unique ability to replicate themselvesin the computer system and spread rapidly from one computer to another affecting file, documents andprograms to alter their normal running . Just like thespread of viruses in human population with an analogythat the individual persons being infected being a terminal, a node or an edge. Similarly, computers can be viewed as terminals in a network that can be infectedwith viruses from one computer node through to another via a network or any connection while sharing resourceor infected data.

Alun L. Lloyd, Robert M. [3] Deliberated computer virus spread analogy by comparing it to human disease spread where individuals (computers) are viewed as nodes of contact. Spafford deduced that viruses are represented as patterns of computer instructional codes [4] that exist over time in computer systems. The viruses like all functional computer codes, are manifestations of algorithms representing an underlying pattern. He further postulated that the patterns of the viruses were to be viewed as a temporary set of electrical and magnetic field changes in thememory or storage of computer systems [5].

Antiviruses [6] on the other hand are programs specially developed to counter challenges brought about by viruses, they protect the computer systems from virus attacks by heavily relaying on the controls enhanced in their databases. Kephart et.al stated that antiviruses-generic virus-detection programs monitor computer system for virus-like behavior Kumar et.al indicated that the antivirus program perform certain actions in protecting the computer systems, they open files, read information in them, openarchives to scan them.

The antiviruses scan the computer using some specific patterns of bytes indicative of known viruses. To stay current, they must be developers of these Antiviruses update their databases whenever new viral Strains arise. Computer virus scanners use pattern matching algorithms to scan for many different signatures at the same time the best checking up to 10,000 signatures in 10,000 programs in less than 10 Minutes Computer security [7] is the protection of information systems from theft or damage to the hardware, and the software. It is also known as cyber security or IT security. It includes controlling physical access to the hardware. It is used as well as protecting against harm that may come via network access, data and code injection. Due to malpractice by operators, whether intentional, accidental, or due to them being into deviating from secure procedures. The field is of growing importance due to the increasing reliance on computer systems in most societies. Computer systems now include a very wide variety of "smart devices. It includes smartphones, televisions and tiny devices as part of the Internet of Things – and networks include not only the Internet and private data networks, but also Bluetooth, Wi-Fi and other wireless networks.

Virus

A computer virus is a small program written to alter the way a computer operates, without the permission or knowledge of the user. A virus must meet two criteria:

- It must execute itself. It will often place its own code in the path of execution of another program.
- It must replicate itself.

For example, it may replace other executable files with a copy of the virus infected file.[8] Viruses can infect desktop computers and network servers alike. Some viruses are programmed to damage the computer by damaging programs, deleting files, or reformatting the hard disk. Others are not designed to do any damage, but simply to replicate themselves and make their presence known by presenting text, video, and audio messages. Even these benign viruses can create problems for the computer user. They typically take up computer memory used by legitimate programs. As a result, they often cause erratic behavior and can result in system crashes. In addition, many viruses are bug-ridden, and these bugs may lead to system crashes and data loss.

Antivirus

The term "antivirus software" stems from the early days of computer viruses, in which programs were created to remove viruses and prevent them from spreading. However, over the years, different types of malicious software, often called malware, emerged as threats to personal and work computers worldwide. Although antivirus software evolved to combat new malware, the term "antivirus" stuck, even though the term antimalware is truer to the software's capabilities. To give us an idea of the different types of malware out there, we've identified malware types that are potential threats to computer systems today. "Antivirus" is protective software designed to defend our computer against malicious software. Malicious software or Malware includes: viruses, Trojans, key loggers, hijackers, dialers, and other code that vandalizes or steals our computer.

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 7, July 2022

Antivirus software is the entry-level version of virus protection for our PC. All antivirus software tools to block or remove spyware, worms, root kits and other malware types. Rather, this particular set of virus protection software has fewer features than the two antivirus suites. This software does include the ability to scan incoming email for potential threats, automatically clean or quarantine infected files, and create bootable rescue disks, to name a few of itsmany features.

A virus definition is binary pattern (a string of ones and zeros) that identifies a specific virus. By checking a program or file against a list of virus definitions, antivirus software can determine if the program or file contains a virus. Most antivirus and Internet security programs reference a database of virus definitions when scanning files for viruses. This is an effective way to detect known viruses. However, when new viruses are created, antivirus software may not recognize them. Therefore, most antivirus programs automatically update the virus definitions from an online database on a regular basis (such as once a week). Some antivirus programs use known virus definitions to generate heuristics that can detect unknown viruses. These viruses may not match a virus definition exactly, but they may be similar enough that the antivirus software can mark the file as a possible virus. While this offers extra protection against unknown viruses, it can also produce "false positives," labeling files as potentially harmful when they do not contain viruses. The accuracy of antivirus heuristics is improved over time based on the feedback end users and developers provide to antivirus software companies. This feedback is used to whitelist or blacklist certain files. By combining this information with up-to-date virus definitions, antivirus software can produce less false positives, yet still catch actual viruses. the pattern file is a database containing information allowing antivirus software to identify viruses. With the exponential growth in malware, the size and frequency of updating the pattern file are becoming increasingly challenging. More and more malware detection will occur in-the-cloud to improve efficiency and efficacy.

Antivirus software was originally developed to detect and remove computer viruses, hence the name. However, with the proliferation of other malware, antivirus software started to protect from other computer threats. In particular, modern antivirus software can protect users from malicious browser helper objects (BHOs), browser hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraud tools, adware, and spyware. Some products also include protection from other computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, advanced persistent threat (APT), and botnet DDoS attacks.

2. DISCUSSION

Computer virus analysis[9] has some common patterns that lend efficiency to the analysis process. In order to stay far from the anti-virus scanners, computer viruses gradually through patters improve their codes to make them invisible. Simply put, computer virus patterns also referred to as virus signatures for those known byantiviruses are means through which viruses replicate themselves over and over as they infect computer systems. Virus signature is the representative byte- pattern part of virus family, which when a virus scannerrecognizes it in a file, it notifies the user that the file is infected.

According to computer Hope, a virus signature is the fingerprint of a virus. It is a set of unique data, or bits of code, that allow it to be identified varietyof viruses may have the same virus

signature allowing anti-virus programs to detect multiple viruses when looking for a single virus signature. Because of this sharing of the same virus signature between multiple viruses, anti-virus programs can sometimes detect a virus that is not even known yet. Typically new viruseshave a virus signature that is not used by other viruses,but new "strains" of known virus sometimes use the same virus signature as earlier strains.

Computer virus authors and antivirus vendors have constantly fought in an evasion of detection game through creation of new virus signatures. Computer malwares have become more and more sophisticated, using advanced code obfuscation techniques to resist antivirus detection. Polymorphic and metamorphic computer viruses are currently the hardest kinds of viruses to detect. Both types of viruses are able to mutate into an infinite number of functionally equivalent.

Anti-Virus Detection Schemes

For antiviruses, a signature is an algorithm or hash that uniquely identifies a specific virus. Depending on the type of scanner being used, it may be a static hash which, in its simplest form, is a calculated numerical value of a snippet of code unique to the virus. Javier stated that a virus signature shouldbe understood how a reliable way to detect a host infected by concrete malware. It encapsulates the essence of a virus. Signature detection is complex and challenging but we will keep the focus on the need of gathering a simple signature together with related context information. With the many antiviruses in the market today, various mechanisms have been employed by them to detect and manage viruses for instance with static analysis, a virus is detected by examining the files or records for the occurrences of virus patterns without actually running any code. Static Methods include the following methods.

The ant-virus software's usually scans files or your computer's memory for certain patterns that may indicate the presence of malicious software's such as viruses. They therefore look for presence of patterns based on the signatures or definitions of known malware. The virus pattern available on a client computer depends on the scan method the client is using. According to a publication by IBM on the Trend Micro Pattern Files and Scan Engine (2015). The Virus Pattern contains information that helps Core Protection Module identify the latest virus/malware and mixed threat attacks. Traditional antivirus software relies heavily upon signatures to identify malware. Substantially, when a malware arrives in the hands of an antivirus firm, it is analysed by malware researchers or by dynamic analysis systems. Then, once it is determined to be a malware, a proper signature of the file is extracted and added to the signatures database of the antivirus software.

Although the signature-based approach can effectively contain malware outbreaks, malware authors have tried to stay a step ahead of such software by writing "oligomorphic", "polymorphic" and, more recently, "metamorphic" viruses, which encrypt parts of themselves or otherwise modify themselves as a method of disguise, so as to not match virus signatures in the dictionary. Antivirus software has some drawbacks, first of which that it can impact a computer's performance. Furthermore, inexperienced users can be lulled into a false sense of security when using the computer, considering their computers to be invulnerable, and may have problems understanding the prompts and decisions that antivirus software presents them with. An incorrect decision may lead to a security breach. If the antivirus software employs heuristic detection, it must be fine-tuned to minimize misidentifying harmless software as

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 7, July 2022

malicious (false positive).

Antivirus software itself usually runs at the highly trusted kernel level of the operating system to allow it access to all the potential malicious process and files, creating a potential avenue of attack. The US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ) intelligence agencies, respectively, have been exploiting anti-virus software to spy on users. Anti-virus software has highly privileged and trusted access to the underlying operating system, which makes it a much more appealing target for remote attacks. Additionally anti-virus software is "years behind security-conscious client-side applications like browsers or document readers.

For most antiviruses in the market today, the most common form of detection of viruses is a heuristic-based detection that use algorithms to compare the signature or patterns of known viruses against a potential threat. The heuristic-based detection allows the antiviruses to detect viruses that have not yet been discovered or previous viruses that have been modified or disguised and released as a new virus. This detection method is the best-known method for detecting new viruses but at times it also generates false positivematches meaning an antivirus scanner may report a file as being infected that is not infected. Further still, computer hope publication indicates that every antivirus scanner has a virus definition file, database, or dictionary that contains thousands of known virus signatures. These signatures allow an antivirus program to identify past viruses that have been analyzed by security professionals. For this another virus detection method includes the signature-based detection approach. This is an excellent way to prevent past known viruses and is best method of detection without creating a false warning. However, signature-based detection cannot detect new viruses until the definitionfile is updated with new virus information.

Other types of antiviruses[10] employ behavior based detection mechanism to detect viruses. This is a unique string of bits, or the binary pattern, of a virus. The virus signature is like a fingerprint in that it can be usedto detect and identify specific viruses. Anti-virus software[6] uses the virus signature to scan for the presence of malicious code. Behavior-based intrusion detection techniques assume that an intrusion can be detected by observing a deviation from normal or expected behaviorof the system or the users.

3. CONCLUSION

Does increased security provide 100% assurance to technology consumers? With the Internet as a major essential communication between billions ofpeople and also a tool for commerce, social interaction,there are increasingly new threats in viruses as new unrecognized signatures are evolving for the antiviruses to detect during the scan. Anti-virus software uses a virus signature to find a virus in a computer file system,allowing detecting, quarantine and removing the virus. In the anti-virus software, the virus signature is referred to as a definition file or DAT file.

Anti-virus software performs frequent virus signature, or definition, updates. These updates are necessary for the software to detect and remove new viruses. New viruses are being created and released almost daily, which forces anti-virus software to need frequent updates. The ability to detect heuristically or generically is significant, given that most scanners now include in excess of 250k signatures and the number ofnew viruses being discovered continues to increase dramatically year after year. Further Landsman indicates that to maintain the

highest level of protection, configure your antivirus software to check for updates as often as it will allow. Keeping the signatures up to date doesn't guarantee a new virus will never slip through, butit does make it far less likely.

REFERENCES:

[1] F. Cohen, "Computer viruses. Theory and experiments," *Comput. Secur.*, 1987.

[2] X. Liu, W. Liu, Y. Liu, H. Song, A. Liu, and X. Liu, "A trust and priority based code updated approach to guarantee security for vehicles network," *IEEE Access*, 2018.

[3] A. L. Lloyd and R. M. May, "How viruses spread among computers and people," *Science*. 2001.

[4] Y. S. Roh and S. S. Kim, "The effect of computer-based resuscitation simulation on nursing students' performance, self-efficacy, post-code stress, and satisfaction," *Res. Theory Nurs. Pract.*, 2014.

[5] V. A. Kotel'nikov and A. V. Shestakov, "Computer systems," *Tyazheloe Mashinostr.*, 1995.

[6] F. H. Hsu, M. H. Wu, C. K. Tso, C. H. Hsu, and C. W. Chen, "Antivirus software shield against antivirus terminators," *IEEE Trans. Inf. Forensics Secur.*, 2012.

[7] L. L. Wear and J. R. Pinkert, "Computer security.," *J. AHIMA*, 1993.

[8] S. Shah, H. Jani, S. Shetty, and K. Bhowmick, "Virus Detection using Artificial Neural Networks," *Int. J. Comput. Appl.*, 2013.

[9] P. Qin, "Analysis of a model for computer virus transmission," *Math. Probl. Eng.*, 2015.

[10] G. Kaur, G. N. Khalsa, and B. S. Dhesian, "Network security : anti-virus," *Int. J. Adv. Res. Comput. Sci.*, 2016.