Review of Viruses and Antivirus Patterns

Yusuf Muchelule
umma university
19 PUBLICATIONS **63** CITATIONS

Neyole Misiko
Umma University
14 PUBLICATIONS **34** CITATIONS

Global Journal of Computer Science and Technology: C
Software & Data Engineering
Volume 17 Issue 3 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Review of Viruses and Antivirus Patterns

By Muchelule Yusuf Wanjala & Neyole Misiko Jacob

Jomo Kenyatta University

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 hand are programs specially developed to counter challenges brought about by viruses as they protect the computer 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.

Keywords: viruses, antiviruses, patterns.

GJCST-C Classification: D.4.6 K.6.5

Review of Viruses and Antivirus Patterns

Muchelule Yusuf Wanjala [α] & Neyole Misiko Jacob [σ]

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 hand are programs specially developed to counter challenges brought about by viruses as they protect the computer 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.

Keywords: viruses, antiviruses, patterns.

I. Introduction

Computer viruses are executable code programs that have a unique ability to replicate themselves in the computer system and spread rapidly from one computer to another affecting file, documents and programs to alter their normal running [1]. Just like the spread of viruses in human population with an analogy that 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 infected with viruses from one computer node through to another via a network or any connection while sharing resource or infected data.

Alun L. Lloyd, Robert M. [2] deliberated computer virus spread analogy by comparing it to human disease spread where individuals (computers) are viewed as nodes of contact. Spafford [3] deduced that viruses are represented as patterns of computer instructional codes that exist over time in computer systems. The viruses like all functional computer codes, are manifestations of algorithms representing an underlying pattern [3]. He further postulated that the patterns of the viruses were to be viewed as a temporary set of electrical and magnetic field changes in the memory or storage of computer systems.

Antiviruses 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 [4] stated that antiviruses- generic virus-detection programs monitor computer system for virus-like behavior [4]. Kumar et.al [5] indicated that the antivirus program perform certain actions in protecting the computer systems, they open files, read information in them, open archives to scan them [5].

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 [4].

II. Computer Virus Patterns

Computer virus analysis 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 by antiviruses 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 scanner recognizes it in a file, it notifies the user that the file is infected [6].

According to computer Hope [7], 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 variety of 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 viruses have 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

Author α σ: Jomo Kenyatta University of Agriculture and Technology.
e-mails: ymuchelule@gmail.com, Jneyole434@gmail.com

copies of themselves [8]. This sophistication comes with the creation of new virus patters that are not easily detectable by the antiviruses available in the market today.

Heuristic detection is a scanning mechanism that anti-virus software employs in detecting for virus signatures. The heuristic detection methods encompass more than 250,000 new virus signatures and are most effective for locating new virus signatures. When there are new signatures created each time a new virus comes out these then should be detect during the virus scans since it is necessary to create the new signatures as the new viruses cannot otherwise be detected[9].

Metamorphic type of viruses modify their code to produce an equivalent one during their propagation. These viruses attempt to evade detection through static analysis by implementing code obfuscation techniques. A technique implemented by swapping interchangeable instructions, inserting garbage instructions and introducing conditional jumps to produce the child virus. Here the signature of a virus is broken by changing the order of instructions without altering the control flow. A sophisticated type of this virus will generate code based on the host's operating system by translating the instructions to the corresponding machine code[10].The detection of these viruses using their signature is challenging since the signature is broken in each version of the virus. In order to detect such metamorphic viruses, the detection system should be designed to extract the essential instructions of the virus from virus instance. This extracted instruction set should be used to detect the viruses of that type [11].

III. 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[12].Javier [13] stated that a virus signature should be 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 [14].

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 [15].

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.

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 generate false positive matches 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 definition file is updated with new virus information [7].

Other types of antiviruses 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 used to detect and identify specific viruses. Anti-virus software 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 behavior of the system or the users[16].

IV. Conclusions

Does increased security provide 100% assurance to technology consumers? With the Internet as a major essential communication between billions of people 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 to detect, quarantine and remove 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 of new viruses being discovered continues to increase dramatically year after year[12]. Further Landesman 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, but it does make it far less likely.

References References Referencias

1. The Journal. (2004, 04 01). Computer Virus Protection. Retrieved from https://thejournal.com/articles/2004/04/01/computer-virus-protection.aspx
2. Alun L. Lloyd, R. M. (18th May 2001). How Viruses Spread Among Computers and People. *Science, New Series*, pp. 1316-1317.
3. Spafford, E. H. (1994). Computer Viruses as Artificial Life. Journal of Artificial Life, MIT Press, pp.1-23.
4. Jeffrey Kephart, Gregory Sorkin, David Chess, Steve White. (Novemnber, 1997). Fighting Computer Viruses. USA: Scientific American.
5. Deepak Kumar, Narender Kumar, Aditya Kumar. (2014). Computer Viruses and Challenges for Anti-virus Industry. International Journal Of Engineering And Computer Science, pp.3869-3873.
6. CTEK-Solutions. (2017, February 10th). Methods of Computer Virus. Retrieved from Ticket Support and Knowledgebase: http://www.ctek-solutions.co.uk/support/knowledgebase.php?article=40
7. Computer Hope. (2017, April 25th). How does an antivirus work? Retrieved from Computer Hope: http://www.computerhope.com/issues/ch001738.htm
8. Serge Chaumette, O. L. (2012). Automated Extraction of Polymorphic Virus Signatures using Abstract Interpretation. France: University of Bordeaux.
9. Techopedia Inc. (2017, April 24th). Virus Signature. Retrieved from Techopedia Inc: https://www.techopedia.com/definition/4158/virus-signature
10. IDA Pro. (2015, May 27th). Retrieved from IDA: https://www.hex-rays.com/products/ida/index.shtml
11. Venkatachalam, S. (May, 2010). DETECTING UNDETECTABLE COMPUTER VIRUSES. Washington Sq: San Jose State University.
12. Landesman, M. (2016, October 20). What is a Virus Signature? Retrieved from Lifewire Tech: https://www.lifewire.com/what-is-a-virus-signature-153629
13. Mellid, J. M. (2014, April 19th). Detecting and removing computer virus with OCaml. Retrieved from http://javiermunhoz.com/blog/2014/04/19/detecting-and-removing-computer-virus-with-ocaml.html
14. Mellid, J. M. (2014, April 19th). *Detecting and removing computer virus with OCaml*. Retrieved from http://javiermunhoz.com/blog/2014/04/19/detecting-and-removing-computer-virus-with-ocaml.html
15. Essam Al Daoud, I. H. (2008). Computer Virus Strategies and Detection Methods. Int. J. Open Problems Compt. Math, pp.122-130.
16. Debar, H. (2017, April 24th). What is behavior based Intrusion Detection? Retrieved from The SANS Institute: https://www.sans.org/security-resources/idfaq/ what- is- behavior- based- intrusion-detection/2/6

This page is intentionally left blank