IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Advancement in Antivirus

Priya Upadhyay[1], Ayushi Saxena[2], Ankuj Singh[1], Pradeep Sharma[3]

Student at Vivekananda College of Technology & Management, Aligarh, India[1]

Lecturer in CS dept. in Vivekananda College of Technology & Management, Aligarh, India[2, 3]

Abstract: Antivirus is a program that identified and removed a particular type of malware that is known as VIRUSES. But in day today life, the working area has increased and now antivirus programs are useful for preventing infections caused by many types of malware, including worms, Trojan horses, root kits, spyware, key loggers, ransom ware and adware. As all antiviruses available in market works on same technology, therefore it seems like even the most up-to-date malware package isn't always enough. The major problems associated with today's antivirus technology are, "That your antivirus software has not yet been updated to know how to detect it" and "your system application software has not been yet patched to fix whatever vulnerability the virus exploits" .The most popular antivirus applications on the market are rendered useless by around 80percent of new malware, according to AusCERT. Most important function of any antivirus is virus scan engine. It scans the information and if the viruses are detected, it disinfects them. The information can be scanned in different ways like through size, pattern matching, heuristic. These methods have their pros and cons. If the antivirus program uses virus signature mechanism then it must update it at least once a day because 15 new viruses we discovered every day. If an antivirus left for two or more days without updating it cause a serious danger. so new advancement in needed into the antivirus to make it advance antivirus (AAV).This paper involves some new techniques which would not only cure pre-existing malicious files, but also all those unseen new malicious file.

Keywords: sandbox, AAV (advance antivirus), heuristic, signature.

I. INTRODUCTION

An anti-virus software program is a computer program that can be used to scan files to identify and eliminate computer viruses and other malicious software (malware). Macro viruses, arguably the most destructive and widespread computer viruses, could be prevented far more inexpensively and effectively, and without the need of all users to buy anti-virus software, if Microsoft would fix security flaws in Microsoft Outlook and Microsoft Office related to the execution of downloaded code and to the ability of document macros to spread and wreak havoc. User education is as important as anti-virus software; simply training users in safe computing practices, such as not downloading and executing unknown programs from the Internet, would slow the spread of viruses, without the need of anti-virus software. According to the research, the best antivirus is not providing the full security, and the reason behind this is that, the soul of antivirus that is his "scan engine" works using 3 main techniques that are size, pattern matching and heuristic.

(a)Size: it can easy detect if the file is infected or altered. Some viruses append their malicious code at the end of the file. An antivirus scanner (scan engine) scans it and compares it before and after sizes. If there is no modification done by the user so it suspects that there is some malicious activity running.

(b)Pattern Matching: In the virus dictionary approach, when the anti-virus software examines a file, it refers to a dictionary of known viruses that have been identified by the author of the anti-virus software. If a piece of code in the file matches any virus identified in the dictionary, then the anti-virus software can then either delete the file, quarantine it so that the file is inaccessible to other programs and its virus is unable to spread, or attempt to repair the file by removing the virus itself from the file. Signature-based detection uses key aspects of an examined file to create a static Finger print of known malware. The signature could represent a series of bytes in the file. This method of detecting malware has been an essential aspect of antivirus tools since their inception, it remains a part of many tools to date, though its importance is diminishing. A major limitation of signature-based detection is that, by itself, this method is unable to flag malicious files for which signatures have not yet been developed. With this in mind, modern attackers frequently mutate their creations to retain malicious functionality by changing the file's signature.

(c)Heuristic: Heuristics-based detection aims at generically detecting new malware by statically examining files for suspicious characteristics without an exact signature match. For instance, an antivirus tool might look for the presence of rare instructions or junk code in the examined file. The tool might also emulate running the file to see what it would do if executed, attempting to do this without noticeably slowing down the system. A single suspicious attribute might not be enough to flag the file as malicious if any information being scanned is dangerous and without knowing that is it contains a virus or not? This method is known as heuristic scanning. It analyze that how an information acting and comparing it with the list of dangerous activities.

Now according to research 98% of the android is under virus infection. The main source of virus is internet. The

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

android play store have 1.5 million apps in total & studies say that their are more than 10 millions of virus exist today. While downloading apps the virus enters into the system. Now another research says that every day 15 new virus comes into spot, so as the antivirus is identifying through signature, then this new virus would not be in the signature list and here this antivirus fails, but though they provide regular update but till then may be you are infected.

II. WORKING OF ADVANCE ANTIVIRUS

Malware authors are in a constant cat-and-mouse game with antimalware researchers. As soon as either makes an advance, the other counters it. So to cure this we need some other techniques other than those traditional ones. The concept involved in AAV is, that there are more virus in the computational world then the useful files. So from decades the antivirus is following the virus in order to cure it. But what if we just allow the useful files in the system to run and denying all other files, so to implement this concept the new advance antivirus (AAV) would be helpful. The advance antivirus would be the mixture of old antivirus + new advancement. As virus is not a application it is just a block of code, which can be either attached or can separately form a program, for some purpose.

This AAV would work in 2 phases:
1. Size
2. Sand box

FIRST PHASE

SIZE: The primary motive would be to allow only those file to run in the system which are verified from original vendor. If a user wants to download a setup of a software than the antivirus would verify weather original vendor had provided the setup of same size which the user in downloading, otherwise block it.

Here we have to consider the proxy based scanning(a known technique), because in that the file size changes so the AAV would have to consider the maximum size threshold.

Proxy based scanning is the best way to prevent malware from being passed into the secured area of the network is to scan any given file in its entirety to ensure it is free from malware. Complete file inspection, often known as proxy-based scanning, can detect malware, which is using evasion methods such as polymorphism and encryption. This requires the gateway system to cache the entire file, decrypt it if necessary, and then inspect it for malware. In this scenario, the size of the file being transferred over the network has a direct effect on the observed network performance. Users typically notice that the file arrives very quickly at the destination after an observed delay. The delay introduced by the caching operation can grow as the file size grows, which administrators interpret as performance degradation.

This scanning method accelerates the file scanning by inspecting only the portion of the file within a single packet and does not wait for the remaining packets to complete the file assembly and caching process. End users will see faster file download speed as scanning occurs during the download. However, since the inspection engine never has a complete view of the file, malicious code or software can be harder to detect with stream based detection. The 10 MB default value has been determined to offer the best possible balance between protection and network performance. As the file size limit is reduced, the rate of detection decreases too.

Now considering the delays and limit, the allowed limit would be set in AAV first phase & the file would pass through the system only if it satisfy the above criteria. Here itself most of the malicious file would be blocked.

The table below shows the percentage of the effectiveness of detection by file size (in MB) limit scanned for each malware type.

	File Size limit										
	1	2	3	4	5	6	7	8	9	10	no limit
exploit	99.83%	99.95%	99.97%	99.97%	99.98%	99.98%	99.99%	100.00%	100.00%	100.00%	100.00%
im-worm	98.83%	99.71%	99.90%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
mass-mailer	99.62%	99.87%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
mobile	99.44%	99.78%	99.88%	99.90%	99.93%	99.95%	99.97%	99.98%	99.99%	99.99%	100.00%
macro virus	99.63%	99.82%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
phish	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
scripts	98.25%	99.64%	99.88%	99.92%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
spyware	95.08%	97.97%	98.88%	99.47%	99.76%	99.83%	99.89%	99.91%	99.94%	99.95%	100.00%
trojan	97.02%	99.24%	99.62%	99.80%	99.88%	99.93%	99.95%	99.97%	99.98%	99.98%	100.00%
virus	98.27%	99.37%	99.63%	99.80%	99.89%	99.92%	99.95%	99.97%	99.98%	99.99%	100.00%
worm	99.02%	99.65%	99.74%	99.86%	99.89%	99.92%	99.94%	99.94%	99.95%	99.96%	100.00%

DOI 10.17148/IJARCCE.2016.52101

SECOND PHASE:

SAND BOX: A sandbox is a testing environment, in which developers "check out" a copy of the source code tree, or a branch thereof, to examine and work on. So we can use this virtual environment to run an application on trial basis. If a file pass through the first phase, it will be tested in second phase. This sand box would be the virtual environment, it will behave and look like as the computer internal architecture and run the application like as it is in real. If the file is a virus file than the AAV would forcefully terminate that sandbox, and the entire system would remain unaffected, and then would empty the entire sand box. Here the user can also delete the file form sandbox in case he found problems in a file, otherwise from the heuristic technique, sandbox would identify the behavior of the file, and if found it a malicious file than would stop the application and delete it. This would clearly determine whether a file is safe for system or not. And if nothing happens and the application runs properly then it would be passing to the system. The area allocated for this testing would be separated through the entire system registry, and other important file. If in case there will be any effect it will be in that bare memory area.

III. CONCLUSION

AS An antivirus tool is an essential component of most antimalware suites. It must identify known and previously unseen malicious files with the goal of blocking them before they can cause damage. This technique of AAV would not only help in blocking the pre-existing virus & malicious files but would also block the unseen malicious file. "The system would just run those files which would pass both the security checks only. When no other file would run in the system then you will be having a forever safe system". This can be the forever cure for this virus problem. In an ideal scenario, all files passing through the network should be scanned to attain the best possible protection (through proxy based scanning). As per statics few virus like Melissa, iloveyou, code red, nimda ,sql slammer, mydoom, conflicker etc. had done a loss of more than 75 billion, so if only 7 virus can do this much loss, what those millions had done. So now it's a time to change the working of antivirus, and make it an advance antivirus (AAV).

ACKNOWLEDGMENT

I would like to thank **Pradeep sharma** and **Aayushi saxena** for their extraordinary support in this thesis process, without whom it was impossible to accomplish this end task. His encouragement made it possible to achieve the goal.

REFERENCES

1. http://www.engpaper.net/antivirus-research-papers.htm
2. http://www.findwhitepapers.com/technology/security/anti_virus
3. http://www.extremetech.com/computing/51498-antivirus-research-and-detection-techniques
4. http://searchsecurity.techtarget.com/tip/How-antivirus-software-works-Virus-detection-techniques
5. http://searchsecurity.techtarget.com/answer/How-to-detect-malware-with-changing-file-sizes
6. Optimization of Antivirus Software published on 2007 in Revista Informatica Economica