Comparative Performance Analysis of Anti-virus Software

Noel Moses Dogonyaro(✉), Waziri Onomza Victor, Abdulhamid Muhammad Shafii, and Salisu Lukman Obada

Cyber Security Science Department, School of Information and Communication Technology, Federal University of Technology, Minna, Nigeria
{moses.noel,victor.waziri,shafii.abdulhamid, salisu.obada}@futminna.edu.ng

Abstract. The threats and damages posed by malwares these days are alarming as Anti-virus vendors tend to combat the menace of malwares by the design of Anti-Virus software. This software also has tremendous impact on the performance of the computer system which in turn can become vulnerability for malware attacks. Anti-Virus (anti-malware) software is a computer program used to detects, prevents and deletes files infected by malwares from communicating devices by scanning. A virus is a malware which replicates itself by copying its code into other computer programs or software. It can perform harmful task on affected host computer such as processors time, accessing private information, corrupting and deleting files. This research carry out malware evasion and detection techniques and then focuses on the comparative performance analysis of some selected Anti-Virus software (Avast, Kaspersky, Bitdefender and Norton) using a VMware. Quick, full and custom scans and other parameters were used. Based on the analysis of the selected anti-virus software, the parameters that offers the utmost performance considering malware detection, removal rate, memory usage of the installed antivirus, and the interface launch time is considered the best.

Keywords: Anti-virus; malware · Evasion · Computer scan

1 Introduction

A computer virus can be defined as a software program that is capable of replicating itself to produce a new file that can harm the computer files. The replication by the virus but it requires a host system or somebody to assist in its spread [1]. Computer virus can destroy or hampered the working processes of a computer and hence always result to negative impact to the computer. Software programmes that are used to work against the computer virus are known as antivirus. The antivirus has the capability of scanning all file programmes on the hard drive and comparing the signature with the one found in the database [2]. The antivirus program can identify, avert and erase computer viruses.

S. Misra and B. Muhammad-Bello (Eds.): ICTA 2020, CCIS 1350, pp. 430–443, 2021.
https://doi.org/10.1007/978-3-030-69143-1_33

The impact, behavior and damage on a computer system, network system or data varies. Companies developing antivirus have developed detecting techniques that this antivirus software can apply. These techniques detection include: behavioral, heuristic and the static methods. Malicious software developers use different dodging principles to avoid been detected. The task for antivirus developers appears to be more on a daily because malware are advancing in developing codes that the antivirus find it difficult to detect.

In recent times, there is an increase threats to data that these malware have caused to computer or network systems. Even with the constant threats to the security of data, antivirus companies still claim that their software products are efficient and reliable to handle all forms of malware. Despite all these assurances many organizations, individuals, and corporation systems or network are been attack and infected with virus with the antivirus installed on their systems [3]. To determine the efficiency and effectiveness of these promising antivirus against malware is of great concern. The question that may be ask is, what are the parameters that a user need to use when testing for the performance of any selected antivirus software? To actualize a better test analysis of an antivirus, the user need to know the following: the negative impact of the antivirus software on its host, and the effectiveness of the scanning process. This research work analyze the performance of Anti-virus software and their individual impact on their hosting computer system.

The research is structure this way: Sect. 2 is the review of related literatures, Sect. 3 describes malware detection and evasion techniques, Sect. 4 briefly explain materials and methods used in the experiment, while section is discussion of results.

2 Review of Related Literatures

The study of anti-virus software has attracted many researchers due to the increase cases in cybercrime globally. The research work of [4] analyzed the effectiveness and the defense obtain by Anti-Virus software. In this work, the author used diverse antivirus software to test Uniform Resource Locator (URL) that is infected with a malware. Forty antivirus software were used to test for the infected URL to ascertain for the strength of all the antivirus software.

In the same line of research, [5] carried out the study on the performance and comparative analysis of different antivirus software. The authors used 193 malicious URL pointed to a malware through download. The results showed that many infected URL were unable to compromise some selected computer system and applications just because the system is patched regularly. This suggest that weaknesses that exist in third-party software applications may have been patched and hence unable to upload any malicious payload on the system.

The research work of [6] takes a different approach. The authors carried out performance study of some selected antivirus software which include: McAFee, Avast, Avira, Bitdefender and Norton. The performance investigation was centered on the scanning period. The performance metrics adopted were, full scan, custom scan and quick scan. Bitdefender outperformed the other antivirus. In order to identify the best antivirus software in 2019, [7] performed comparative study on14 anti-virus programs by using

452 live malware samples. The result obtained showed that Bitdefender was the best after 700 h of the test. The parameters used were, the effects of the antivirus on a computer system, protection capability of the malware protection, security of the browsing, and how spam are filtered.

In this research work, four anti-virus software products commonly used in Federal University of Technology, Minna was selected. The selection was based on the results obtained during survey of antivirus software in some selected higher institutions in Niger state including the Federal University of technology, Minna. These include: Avast, Bitdefender, Kaspersky, and Norton. Unlike the work of [7], this research would consider using the following performance metrics for the analysis: quick scan, full scan, custom scan, size of the installed anti-virus, how the processor is used when idle and when performing a scan, memory used when idle state, and the time taken for the antivirus to launch.

3 Malware Detection and Evasion Techniques

Malware (malicious software) as defined by [8] are program codes that can harm a computer system or network. The malicious codes have the tendency of infecting computer files or installed software programmes. The research work of [9] classify malware into the following categories based of their behavioral pattern. These include: Virus, and Worm. Those that their spread does not require human intervention are the Trojan or Trojan horse, Spyware, and the Ransomware. Malware detection techniques can be classify into three basic group: signature based, behavioral based, and the heuristic based [10]. In the signature based technique, searching of different bytes sequences is done so as to recognize particular portion of the malware. While the behavioral-based method, the technique observes the behavior of the computer software to ascertain whether it is harmful or not [10]. The heuristic-based technique try to examine system abnormality behavior. In this technique, constant software update is not necessary [11]. However, it is good to acknowledge that each detection techniques has its weaknesses and strength on the computer resources in which it is implemented.

With the recent proliferation of malware which are used in most cybercrime, Antivirus companies are also writing antivirus codes that could detect and neutralize malware [12]. As the antivirus software companies are making efforts to detect and neutralize these malware, hackers in turn are deploying malware programs that can go undetected, hide or bypass the antivirus programs. Some of the techniques adopted by the malware writers to execute their nefarious acts include: Polymorphism, Oligomorphism, and Metamorphic malware evasion techniques [13].

4 Materials and Methods

Materials: The following materials were used during the experiment: Windows 10 Pro O.S; 4 GB installed memory card, Core i5 CPU with 2.5 GHz processor speed; 64-bit O.S; VMware workstation 12 pro.

Methodology: To start the experiment, the authors first installed the VMware software on the host computer. Thereafter, the windows 10 O.S was also installed on the virtual machine and configured before installing the anti-virus software. Individual performance of each anti-virus software was done using some selected parameters. The parameters selected include: quick scan, full scan, custom scan, installation size of the antivirus, normal processor usage when it is idle, average processor usage during scanning, average memory usage during idle, and anti-virus interface launch time.

The experiment was conducted in a virtual environment. The selected anti-virus software were installed on the windows 10 pro operating system. Each of the antivirus software was used to scan for malware to test for the efficiency. The block diagram for the analysis is shown in Fig. 1.

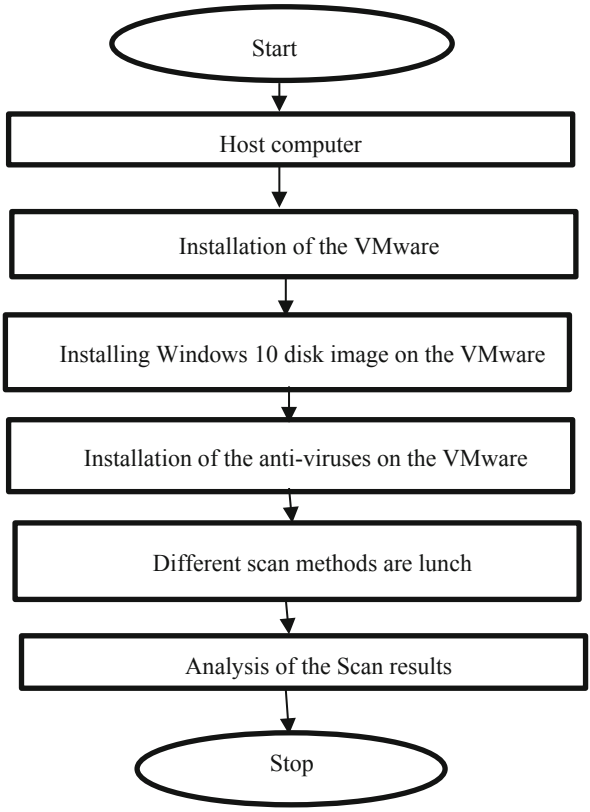

Fig. 1. Block diagram of Installation and scanning process (VMware and the anti-viruses)

5 Discusion of Results

5.1 Performance Measures

Metric 1: Quick Scan

Table 1. Results for the Quick Scan

Anti-virus type	Total files scanned	Time (minutes)
Avast	28887	13
Bitdefender	57	2
Kaspersky	3571	9
Norton	10876	4

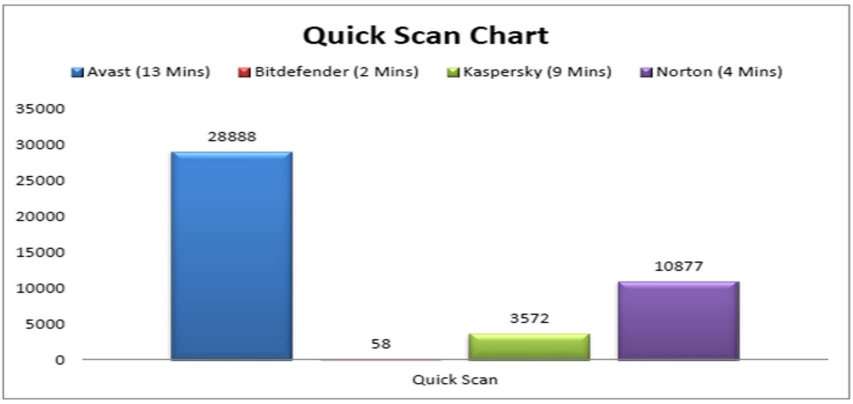

Fig. 2. Quick scan graph scan

Figure 2 represent the graphical of the quick scan. In the graph, the vertical line is the y-axis and it represents the total number of computer files the antivirus was able to scan. Looking at the results, Bitdefender scanned 57 files in the space of 2 min, Kaspersky scanned 3571 files in 9 min, Norton 10876 in 4 min and Avast was able to scan 28887 files in just 13 min. In this result, Avast perform best in terms of number of files scanned. Avast results suggest that no hidden malware would go undetected.

Metric 2. Full Scan

Table 2. Results for the Full Scan

Anti-virus type	All files scanned	Time (minutes)
Avast	260661	43
Bitdefender	333118	49
Kaspersky	129871	14
Norton	159117	44

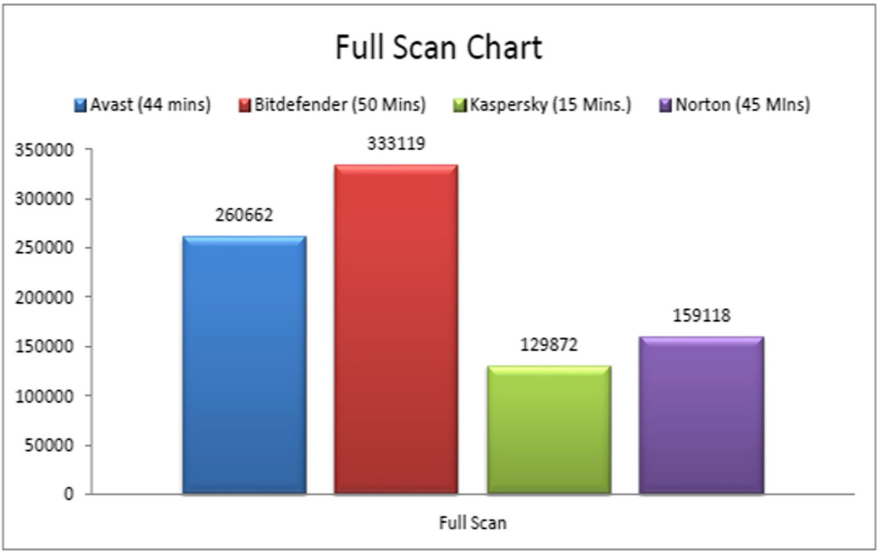

Fig. 3. Full Scan graph

In Fig. 3, it can be seen from the result that Kaspersky scanned 129872 of all files in the system in just fifteen minutes. Norton and Avast scanned 159118 and 260662 files in just 45 and 44 min. Bitdefender was able to scanned 333119 files in fifty minutes. This showed that Kaspersky scanned lesser documents in fewer time when comparing this to Norton anti-virus in which more files where scanned with longer time taken. Avast on the other side scanned more documents taken much time when you are making comparison to Norton. Bitdefender scanned much files with much time than Avast and Norton. Based on the analysis, Bitdefender performs better because of the total number of documents scanned. The scan can reveal hidden malware no matter its location in the computer system.

Metric 3. Custom Scan

Table 3. Results for the Custom Scan

Anti-virus type	Total files scanned	Time (minutes)
Avast	23561	10
Bitdefender	147652	10
Kaspersky	135961	57
Norton	141332	13

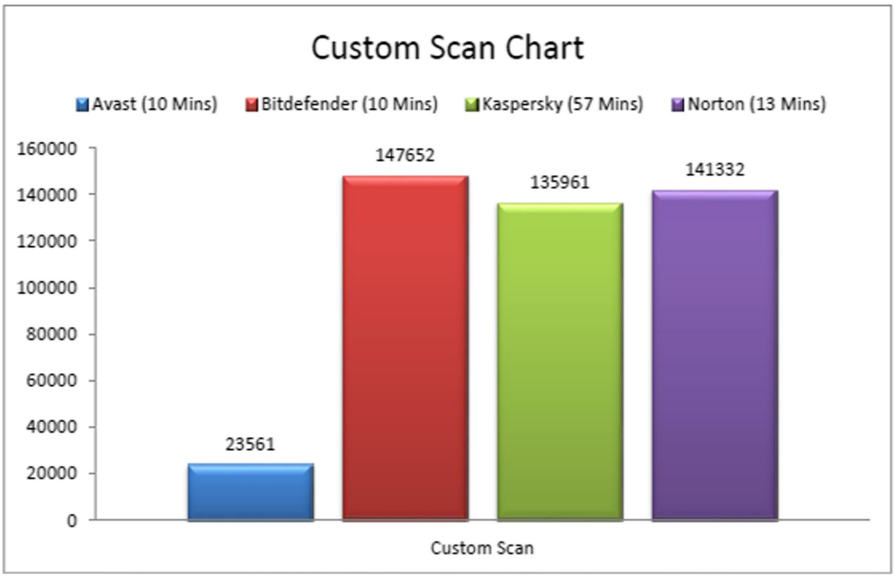

Fig. 4. Chart of the Custom Scan

Figure 4 represents the chart of the custom scan. In the chart, Avast anti-virus software scanned 23562 documents in just 10 min. A total of 135961 documents in 57 min were scanned by Kaspersky. Norton used 13 min to scan 141332 files, and 147652 files were scanned by Bitdefender in 10 min. In this result, Kaspersky scanned few files although the time taken was higher as compare to Norton. Avast total number of files scanned were less and the time was also short as compare to Kaspersky. More documents were scanned by Bitdefender than Avast within the same time frame. Lastly, Bitdefender and Avast scanned more files at the same time interval.

Metric 4. Installation size

Table 4. Custom scan results

Anti-virus type	Size in bytes	Size in (MB)
Avast	1035387855	987
Bitdefender	645437870	615
Kaspersky	284127515	270
Norton	675759587	644

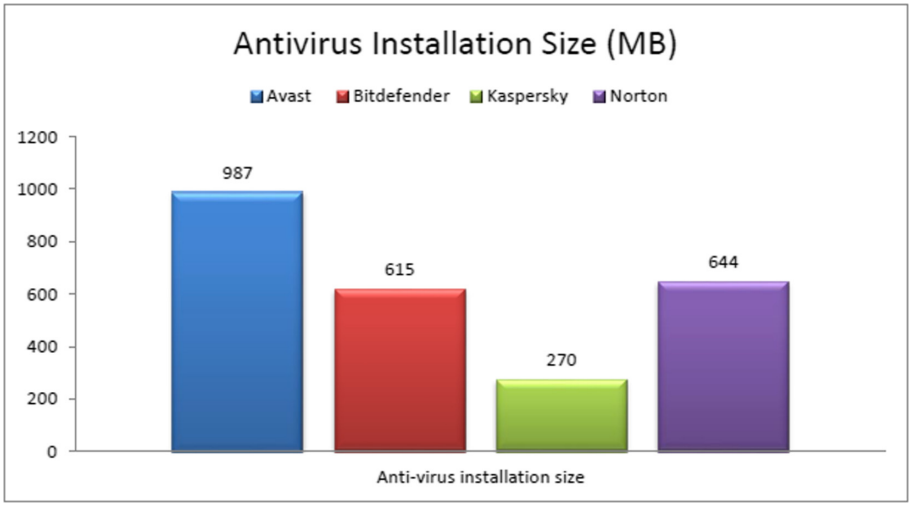

Fig. 5. Anti-virus installation size

Figure 5 is the chart that represent the size of the antivirus when installed on the computer and it is in gigabytes. From the results, Avast has 987 MB on disk, Bitdefender used 615 MB size on disk after installation, Kaspersky used 270 MB and Norton used 644 MB respectively. In this results, Kaspersky occupies less memory space after installation followed by Bitdefender. The memory space any antivirus occupies has a negative or positive impact on the host computer system. The size of the antivirus may slow down the computer system especially during updates installation.

Metric 5. Idle state of the processor usage

Table 5. Custom scan results

Serial No	Type of anti-virus	Ave. Processor usage (%)
1	Avast	0.38
2	Bitdefender	1.07
3	Kaspersky	0.45
4	Norton	0.74

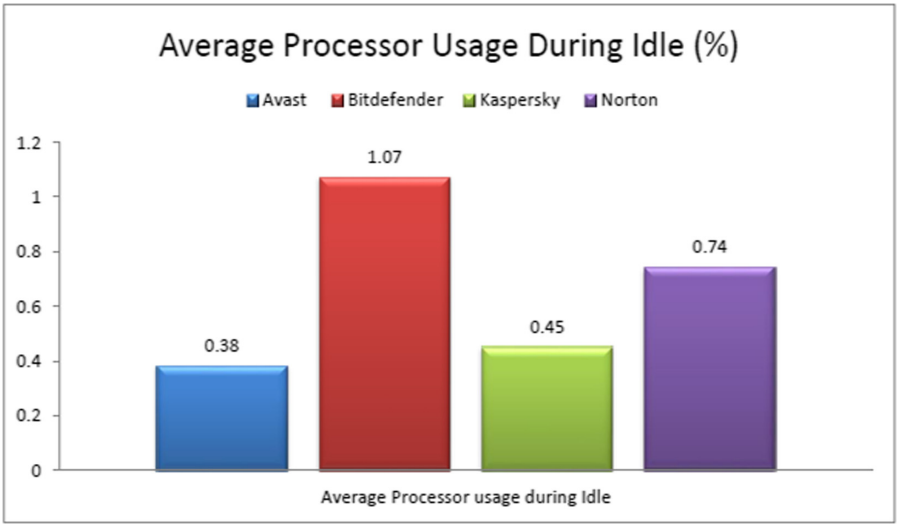

Fig. 6. During idle time average processor usage

Figure 6 is the bar chart representing the idle state of the processor usage. It is recorded in percentage form. From the result, with a 2 GB processor, Avast uses 0.38% of the processing space. Also, 1.07% space was used by Bitdefender, 0.45% processing space by Kaspersky, while 0.74% of the processing space was used by Norton. From the results, it showed that Avast uses less processor when it is in the idle state when compare to the other anti-virus software products. The system performance is impacted negatively or positively. The result also indicates how slowly or fast a system could be. If a system is too slow in executing some basic commands, hackers could take advantage of this limitation to hack into the system or cause Denial of Service attacks.

Metric 6. Result of scanning of Processor Usage

Table 6. Custom scan results (%)

S/N	Anti-virus type	Ave. Processor usage (%)
1	Avast	11.19
2	Bitdefender	16.04
3	Kaspersky	23.58
4	Norton	31.75

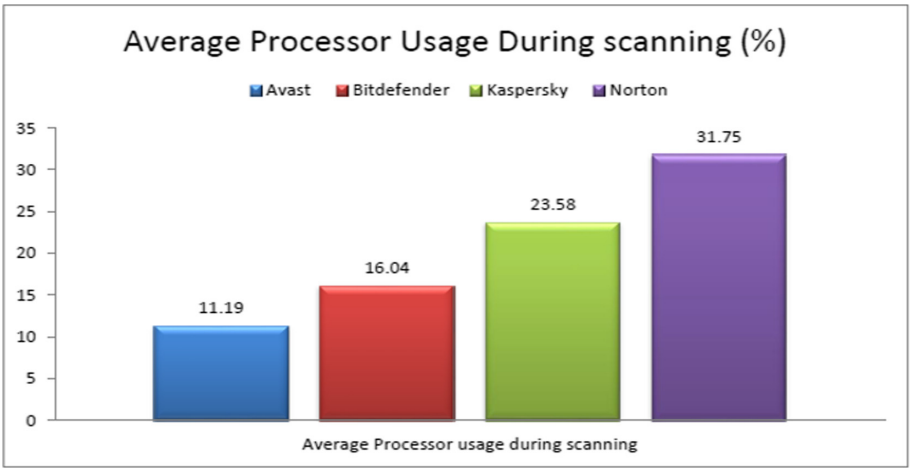

Fig. 7. Average processor usage during scanning

During scanning state, the average processor usage is represented in Fig. 7. From the chart, 11.19% of scanning was used by Avast, while Bitdefender requires 11.06% of the scanning. Kaspersky used 23.58% for scanning while 31.75% of the scanning the computer system was used by Norton. It is proven when an anti-virus software utilize more of the processor memory during scanning, there is this tendency that the system may slow down the system processor thereby affecting other processes. Norton anti-virus software consumes more processor memory than the other anti-virus software. In summary of the result, Avast uses less memory compared to the other anti-virus software. This showed that in terms of average processor usage and memory consumption during scanning, Avast is the best.

Metric 7. Average Memory Usage (Idle state)

Table 7. Custom scan results

S/N	Anti-virus type	Ave. Memory usage KB
1	Avast	41317
2	Bitdefender	131893
3	Kaspersky	47704
4	Norton	11425

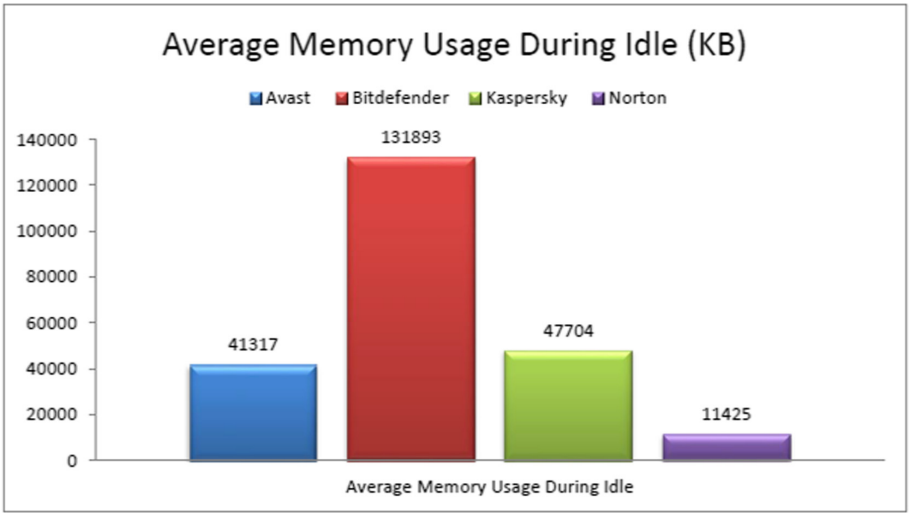

Fig. 8. During idle state memory usage

Figure 8 is the chart of the all the anti-virus software average memory usage while on idle state. The memory usage is measured in kilobytes. The results showed that Bitdefender consumes an average of 131893 KB per minute when the system is in the idle state. Average consumed by Kaspersky is 47704 KB, Avast takes 41317 KB, while on an average of 11425 KB was used by Norton. The analysis of the results showed that more memory usage was required by Bitdefender in idle state while Norton uses less memory when on idle state. When the memory consumption is less, it implies better performance by the system.

Metric 8. Memory Usage during Scanning

Table 8. During scanning average memory usage

S/N	Anti-virus type	Ave. Memory usage in KB
1	Avast	107879
2	Bitdefender	223142
3	Kaspersky	109593
4	Norton	107027

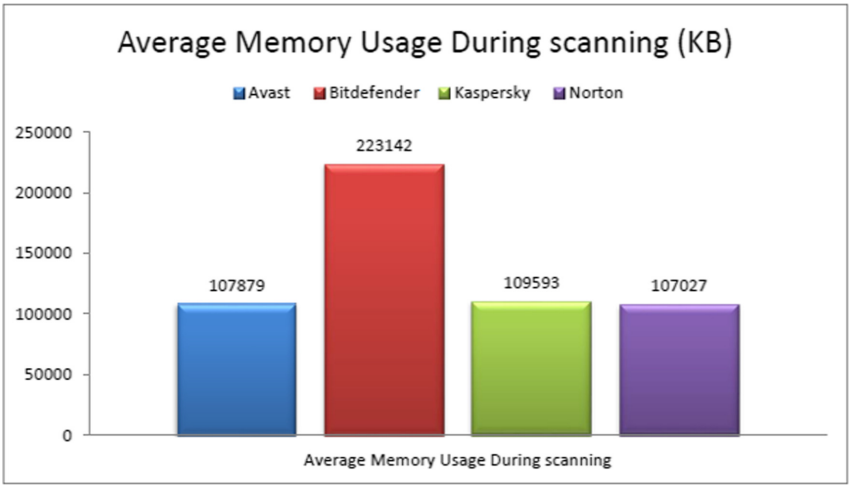

Fig. 9. During scanning- (average memory usage)

During scanning, the average memory usage by all the antivirus software is represented in Fig. 9 and it is measured in kilobytes. From the scanning results, an average of 2231 KB was used by Bitdefender, while 109593 KB of memory was used by Kaspersky. Avast uses an average of 107879 KB, while on average, 107027 KB of memory was used by Norton. It could be concluded that from the result more memory space was used by Bitdefender during scanning of files than Norton antivirus. Using this parameter, it helps in determining the performance of the system and also its efficiency.

Metric 9. The interface launch time.

Table 9. Custom scan results

S/N	Anti-virus type	Ave. Launch Time (milliseconds)
1	Avast	0.4387
2	Bitdefender	–
3	Kaspersky	0.2398
4	Norton	0.1296

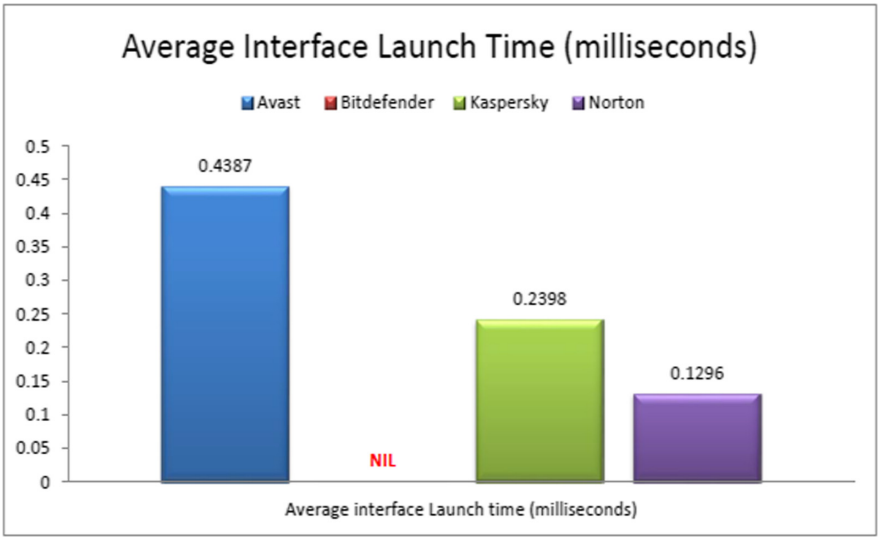

Fig. 10. Anti-virus Interface Launch Time

The average interface launch time of all the antivirus software are represented in Fig. 10. This is measured in milliseconds. In Table 9, The user interface launch time for Avast is in the average of 0.4387 ms, Kaspersky used 0.2398 ms, while 0.1296 ms was taken by Norton for the user interface to be fully launched. There was denial access of interface by the 'apptimer' on Bitdefender. When the time taken to launch the interface is less, it implies better performance by the selected antivirus software. The User Interface response time by any antivirus determines the operability and user friendly the anti-virus should be. Using this parameter indicates that Norton anti-virus User interface launched time is faster as compared to Kaspersky and the other two antivirus software.

6 Conclusion

This research used three (3) basic parameters: quick scan, full scan, and custom scan. To know the time and the total files scanned, the authors used the quick scan method. In order to obtain the time and the total number of scanned documents, the authors applied the full scan method. The effectiveness of an anti-virus was determine by sing the custom scan method. The research also considered the following parameters to determine the performance and effectiveness of the chosen antivirus: the installation size of the antivirus on disk, size of the memory it occupy on the C: drive, the processor usage during scanning and when the system is in its idle state, the average memory usage during scanning and while on ide state, the interface launched time for all the selected antivirus software was calculated. The recommendation that could be made on any antivirus software is based on the parameters that gives the utmost performance as regards to malware detection and removal rate, memory usage of the installed antivirus, and the interface launch time should be consider.

The authors therefore recommend future research of other antivirus software and applying other malware detection techniques. Antivirus vendors should be up to date with the recent trends and techniques used by malware writers to evade detection.

References

1. Gandotra, E., Bansal, D., Sofat, S.: Malware analysis and classification: a survey. J. Inf. Secur. (2014)
2. Barriga, J.J., Yoo, S.G.: Malware detection and evasion with machine learning techniques: a survey. Int. J. Appl. Eng. Res. **12**(18), 7207–7214 (2017)
3. Al-Asli, M., Ghaleb, T.A.: Review of signature-based techniques in antivirus products. In: 2019 International Conference on Computer and Information Science (ICCIS), pp. 1–6. IEEE, Saudi Arabia (2019)
4. Willems, E.: The antivirus companies. In: Cyberdanger, pp. 65–83. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-04531-9_5
5. Johar, A.H., Gerard, A., Athar, N., Asgher, U.: Feature based comparative analysis of online malware scanners (OMS). In: Ayaz, H., Asgher, U. (eds.) AHFE 2020. AISC, vol. 1201, pp. 385–392. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-51041-1_51
6. Alqurashi, S., Batarfi, O.: A comparison of malware detection techniques based on hidden markov model. J. Inf. Secur. **7**(3), 215–223 (2016)
7. Johnston, N.: The best antivirus software for 2018, 25 August 2018. https://www.toptenreviews.com/software/security/best-antivirus-software/. Accessed 28 April 2020
8. Deylami, H.M., Muniyandi, R.C., Ardekani, I.T., Sarrafzadeh, A.: Taxonomy of malware detection techniques: a systematic literature review. In: 2016 14th Annual Conference on Privacy, Security and Trust (PST), pp. 629–636. IEEE, New Zealand (2016)
9. Bai, L., Rao, Y., Lu, S., Liu, X., Hu, Y.: The software gene-based test set automatic generation framework for antivirus software. JSW **14**(10), 449–456 (2019)
10. Al Amro, S., Alkhalifah, A.: A comparative study of virus detection techniques. Int. J. Comput. Inf. Eng. **9**(6), 1566–1573 (2015)
11. Euh, S., Lee, H., Kim, D., Hwang, D.: Comparative analysis of low-dimensional features and tree-based ensembles for malware detection systems. IEEE Access **8**, 76796–76808 (2020)
12. Garba, F.A., Kunya, K.I., Ibrahim, S.A., Isa, A.B., Muhammad, K.M., Wali, N.N.: Evaluating the state of the art antivirus evasion tools on windows and android platform. In: 2019 2nd International Conference of the IEEE Nigeria Computer Chapter (NigeriaComputConf). IEEE, Zaria, Nigeria, pp. 1–4 (2019).
13. Chakkaravarthy, S.S., Sangeetha, D., Vaidehi, V.: A survey on malware analysis and mitigation techniques. Comput. Sci. Rev. **32**, 1–23 (2019)