VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

FACULTY OF ELECTRONICS

DEPARTMENT OF COMPUTER SCIENCE AND COMMUNICATIONS TECHNOLOGIES

Priyanka Wagle

INVESTIGATION AND EVALUATION OF THE IMPACT OF ANTIVIRUS PROTECTION ON THE PERFORMANCE OF A PERSONAL COMPUTER

Master Thesis

Computer Engineering study programme, state code 6211EX051

Computer Engineering specialisation

Electronics Engineering study field

Vilnius, 2024

VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

FACULTY OF ELECTRONICS

DEPARTMENT OF COMPUTER SCIENCE AND COMMUNICATIONS TECHNOLOGIES

Priyanka Wagle

INVESTIGATION AND EVALUATION OF THE IMPACT OF ANTIVIRUS PROTECTION ON THE PERFORMANCE OF A PERSONAL COMPUTER

Master Thesis

Computer Engineering study programme, state code 6211EX051

Computer Engineering specialisation

Electronics Engineering study field

Supervisor Assoc. Prof. Dr. Gediminas Gražulevičius

Vilnius, 2024

VILNIUS GEDIMINAS TECHNICAL UNIVERSITY
FACULTY OF ELECTRONICS
DEPARTMENT OF COMPUTER SCIENCE AND COMMUNICATIONS TECHNOLOGIES

Electronics Engineering study field
Computer Engineering study programme, state code 6211EX051
Computer Engineering specialisation

APPROVED BY
Head of Department
Vaidotas Barzdėnas
2024-05-29

OBJECTIVES FOR MASTER THESIS

No. KTfmu-22–7837

Vilnius

For student Priyanka Wagle

Master Thesis title: Investigation and Evaluation of the Impact of Antivirus Protection on the Performance of a Personal Computer

Deadline for completion of the final work according to the planned study schedule.

THE OBJECTIVES:

The aim of the Master's thesis: The goal of this work is to investigate the impact of the most popular personal computer antivirus programs on the performance of a personal computer, and the performance of basic operations and functions, to evaluate the obtained results and provide recommendations.

The task of the Master's thesis:
In order to achieve the goal, the following tasks must be solved:
1. To review the types of computer threats (viruses, malware, spyware, adware, ransomware, rootkit, spam, botnet, phishing, key logger, etc.) and methods of their detection;
2. To analyze the principles of operation of antivirus programs, their peculiarities and their components;
3. Carry out a questionnaire and highlight the most popular free and paid antivirus programs;
4. To select tests to investigate the impact of antivirus programs on personal computer computer performance, and the performance of basic operations and functions;
5. To experimentally study the impact of the most popular (according to the results of the survey) antivirus programs on the computer performance and the performance of basic operations and functions;
6. Compare the impact of paid and free antivirus programs on computer performance;
7. Conclusions and recommendations.

Academic Supervisor Associated Professor Gediminas Gražulevičius

Vilnius Gediminas Technical University
Faculty of Electronics
Department of Computer Science and Communications Technologies

ISBN | ISSN
Copies No. .....
Date .....-.....-.....

Master Degree Studies **Computer Engineering** study programme Master Graduation Thesis

Title	**Investigation and Evaluation of the Impact of Antivirus Protection on the Performance of a Personal Computer**
Author	**Priyanka Wagle**
Academic supervisor	**Gediminas Gražulevičius**

Thesis language: English

Annotation

As digital threats continue to evolve, the need for effective antivirus protection is paramount to safeguarding personal computers from malicious activities. These antivirus programs also have a tremendous impact on the performance of the computer system, which in turn can become vulnerable to malware attacks. This study delves into the intricate relationship between antivirus software and the overall performance of a personal computer by focusing on the comparative performance analysis of some selected free and paid antivirus software on the same computer. A survey of around 130 respondents was conducted to select antivirus software for testing. The study takes parameters such as the boot time of an operating system, the copying time of a set of files, the working memory used by antiviruses, and various application start-up times to understand the impact of the antivirus program on personal computer performance. The thesis consists of 49 p. text without appendices, 15 figures, and 28 bibliographical entries. Appendices attached.

Keywords: Antivirus software, malware, survey, personal computer performance

Vilniaus Gedimino technikos universitetas
Elektronikos fakultetas
Kompiuterijos ir ryšių technologijų katedra

ISBN | ISSN
Egz. sk. .....
Data .....-.....-.....

Antrosios pakopos studijų **Kompiuterių inžinerijos** programos magistro baigiamasis darbas

Pavadinimas	**Antivirusinės apsaugos įtakos asmeninio kompiuterio greitaveikai tyrimas ir vertinimas**
Autorius	**Priyanka Wagle**
Vadovas	**Gediminas Gražulevičius**

Kalba: anglų

Anotacija

Kadangi skaitmeninės grėsmės ir toliau vystosi, veiksmingos antivirusinės apsaugos poreikis yra itin svarbus siekiant apsaugoti asmeninius kompiuterius nuo kenkėjiškos veiklos. Šios antivirusinės programos taip pat turi didžiulį poveikį kompiuterinės sistemos veikimui, kuri savo ruožtu gali tapti pažeidžiama kenkėjiškų programų atakų. Šiame tyrime gilinamasi į sudėtingą antivirusinės programinės įrangos ir bendro asmeninio kompiuterio našumo ryšį, daugiausia dėmesio skiriant kai kurių pasirinktų nemokamos ir mokamos antivirusinės programinės įrangos tame pačiame kompiuteryje našumo analizei. Buvo atlikta maždaug 130 respondentų apklausa, skirta išbandyti antivirusinę programinę įrangą. Norint suprasti antivirusinės programos poveikį asmeninio kompiuterio veikimui, tyrime naudojami tokie parametrai kaip operacinės sistemos įkrovos laikas, failų rinkinio kopijavimo laikas, antivirusinių programų naudojama darbinė atmintis ir įvairūs programos paleidimo laikai. Darbo apimtis – 49 p. teksto be priedų, 15 paveikslų ir 28 bibliografiniai šaltiniai. Pridėti darbo priedai.

Prasminiai žodžiai: Antivirusinė programinė įranga, kenkėjiškos programos, apklausa, asmeninio kompiuterio greitaveika.

VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

Priyanka Wagle, 20223566

(Student's given name, family name, certificate number)

Faculty of Electronics

(Faculty)

Computer Engineering, KTfmu-22

(Study programme, academic group no.)

DECLARATION OF AUTHORSHIP
IN THE FINAL DEGREE PAPER

May 29, 2024

I declare that my Final Degree Paper entitled „Investigation and Evaluation of the Impact of Antivirus Protection on the Performance of a Personal Computer“ is entirely my own work. I have clearly signalled the presence of quoted or paraphrased material and referenced all sources.

I have acknowledged appropriately any assistance I have received by the following professionals/advisers: Assoc Prof Doctor Gediminas Gražulevičius.

The academic supervisor of my Final Degree Paper is Assoc Prof Doctor Gediminas Gražulevičius.

No contribution of any other person was obtained, nor did I buy my Final Degree Paper.

(Signature)

Priyanka Wagle

(Given name, family name)

Table of Contents

Table of Figures

1. INTRODUCTION

A computer virus is a software program capable of replicating itself to generate a new file, posing a threat to computer files. Replication requires a host system or assistance for spread [1]. Computer viruses can disrupt or impede computer operations, leading to negative impacts. Antivirus software is designed to counteract these viruses, scanning hard drive files, and comparing signatures with a database [2]. The effects, conduct, and damage experienced by computer systems, network systems, or data can differ. Antivirus developers have created detection methods, encompassing behavioural, heuristic, and static approaches [3–5]. Developers of malicious software employ diverse evasion tactics to circumvent detection. Antivirus products might be effective. However, their impact on the performance of the computer system (Host) is something that should also be considered. While antivirus vendors aim to combat the growing threats and damages posed by malware through the design of antivirus software, the same software can inadvertently impact the performance of the computer system. This impact on performance can, in turn, create vulnerabilities that may be exploited by malware attacks. The very measures taken to protect a system from malware can introduce challenges in terms of system performance [6].

With respect to user experience, the performance aspect is crucial because users want an antivirus solution that not only effectively detects and removes threats but also does so without significantly slowing down their system. Our tests are driven by the aim of offering a more tailored perspective, exploring specific aspects not covered in existing tests. By customizing the research focus, testing configurations, and delving into user perceptions, the study seeks to provide a nuanced and valuable contribution to the current understanding of antivirus effectiveness towards computer performance.

1.1. The purpose and tasks of the work

The purpose of the work is to study the impact of the most popular antivirus programs on computer performance and the speed of performing basic actions. In order to achieve the goal, the following tasks were solved:

1. Review the types of computer threats and methods of their detection.

2. Analyze the operating principles, features, and components of antivirus programs.

3. Carry out a questionnaire (about for 100 students) and highlight the most popular free and paid antivirus programs.

4. Select tests to investigate the impact of antivirus programs on personal computer performance, and the performance of basic operations and functions (personal computer boot time, random access memory usage, file set copy time, user program start-up time).

5. Experimentally study the impact of the most popular (according to the results of the survey) antivirus programs on the personal computer performance and the performance of basic operations and functions:

- Quantifying the duration required for computer startup after antivirus program installation.
- Assessing the extent of working memory utilization by the antivirus software.
- Measuring the time necessary for copying a predefined set of files.
- Determining the elapsed time for launching applications subsequent to antivirus program installation.

6. Compare the impact of paid and free antivirus programs on the personal computer performance.

2. COMPUTER THREATS

Computer threats refer to any activity that has the potential to cause harm to a computer system, its data, or its users. These threats can include unauthorised access to data, theft, manipulation, and destruction of data. In simple terms, a computer threat is a potential danger that can exploit vulnerabilities in a system to breach security and cause damage.

In the era where every activity in the real world is digitised, people had to switch from paper documents to online methodologies. When it comes to an individual, the best example would be online banking. The user has no idea what goes in the background when they transfer money, pay bills, shop online, etc. Therefore, as such activities increase and become popular, it is important to follow safe computing and protect user data. In general, practising safe computing involves protecting one's computer hardware and software from unauthorised access or interference by outside parties. Furthermore, computer security also encompasses the protection of personal devices used to access the Internet, such as personal computers, smartphones, routers, and networks. Additionally, it involves securing sensitive personal information, such as names, email addresses, national identification numbers, and credit card numbers, from online threats [7].

It is not just the responsibility of security engineers and organisations to protect our computers and data, but also the users. It is important for the user to understand how to prevent and avoid threats to personal computers and networks.

2.1. Malware and various types

Any piece of software that interferes with computer operation, steals data, gains access to secure networks, or displays unwelcome advertising is called malicious software or malware. Malware damages computers intentionally, directly or indirectly, by corrupting files or by stealing important user data from computers. Software with a defect that inadvertently causes harm is not malware. In the early days, malware was written for simple purposes, thus, it was easier to detect. This kind of malware can be defined as traditional (simple) malware. However, these days, the malware which can run in kernel mode, and is more destructive and harder to detect than traditional malware can be defined as new generation malware (next-generation). This kind of malware can easily bypass protection software that is running in kernel mode such

as firewalls, antivirus software, etc. Malware is created with a variety of objectives in mind, from the minor to the serious, from showing advertisements to destroying or corrupting data to stealing user bank account or credit card information [8].

- **Spyware**: Spyware is harmful software designed to infiltrate your computer, collect information about you, and send it to a third party without your consent. It can also refer to legitimate software that tracks data for business purposes like advertising. However, malicious spyware specifically aims to profit from stolen data.

- **Adware**: Monitors user activity and sells data to advertisers. It often disguises itself as legitimate software or piggybacks on other programs. Adware generates revenue by displaying advertisements, leading to unwanted pop-ups, homepage changes, and fake alerts.

- **Infostealer**: Collects sensitive information from devices, such as login credentials and financial data, and sends it to attackers. Often used in malware-as-a-service, infostealers can also drop additional malware on compromised systems.

- **Keyloggers**: Record every keystroke typed on a device to capture passwords and other sensitive information. While they can be used for legitimate purposes, cybercriminals often use them to steal data.

- **Rootkits**: Allow attackers deep access to a device by exploiting vulnerabilities. Rootkits can hide their presence while stealing data, installing malware, or using the device in botnet attacks.

- **Red Shell**: Installs with certain PC games and tracks online activity. It collects data like operating system, installed browsers, and IP addresses, often for marketing purposes.

- **System Monitors**: Track user activity, capturing keystrokes, emails, websites visited, and programs run. Often disguised as freeware, they record nearly everything a user does on their computer.

- **Tracking Cookies**: Dropped by websites to follow a user's online activity, these cookies collect browsing data for advertisers.

Other malware types:

- **Trojan Horse**: Disguises itself as legitimate software to trick users into installing it. Once inside, it can steal data, install other malware, or disrupt the system.
- **Ransomware**: Restricts access to a computer or files and demands a ransom for their release. It encrypts data and threatens permanent loss if the ransom is not paid.
- **Spam**: Unsolicited digital communication sent in bulk, often through email. It includes phishing emails, email spoofing, tech support scams, and hot topic scams.
- **Botnets**: Networks of infected computers controlled by a single entity, used for DDoS attacks, spamming, and spreading malware.
- **Phishing**: Cyber attacks that trick individuals into providing sensitive information or installing malware through deceptive emails or messages.
- **Worms**: Self-replicating malware that spreads without human intervention, often through networks. Unlike Trojans, worms can independently propagate once inside a system.[11]

2.1.1. Signs of malware on a computer

Identifying signs of malware on a computer is crucial for maintaining cybersecurity. According to insights shared by cybersecurity experts at Malwarebytes, there are several key indicators that may suggest your system has been compromised [9]:

- **Decreased Performance**: If your computer suddenly becomes sluggish, unresponsive, or experiences frequent freezes, it might be a sign of malware consuming system resources in the background.
- **Unwanted Pop-ups and Advertisements**: Malware often generates intrusive pop-up ads, even outside of web browsing sessions. These ads may appear on your desktop or within applications without your consent.
- **Browser Settings Alterations**: Malicious software can tamper with your browser settings, such as changing the homepage, default search engine, or installing unauthorized toolbars and extensions.

- **Abnormal Behavior**: Keep an eye out for unexpected activities like programs launching on their own, your email account sending out spam, or files being accessed without your authorization, as these could indicate malware presence.

- **Security Alerts**: Malware may attempt to disable or interfere with your computer's security software. Be wary of notifications indicating disabled antivirus or firewall programs, which could signal an ongoing malware attack.

- **Unusual Network Activity**: Monitoring your network for unusually high data traffic can help detect malware attempting to communicate with remote servers for malicious purposes.

- **Missing Files or Programs**: If files suddenly disappear or unfamiliar programs appear on your system, it could be a sign of malware deleting or installing files without your knowledge.

- **Frequent System Crashes**: Malware-infected systems may experience frequent crashes or display error messages, suggesting underlying system instability caused by malicious software.

- **Unexplained Disk Activity**: Excessive disk activity, particularly when the computer is idle, may indicate malware performing disk-intensive operations such as file encryption or data theft.

- **Changes in System Settings**: Be vigilant for any unauthorized changes to system settings, such as disabled security features or altered configurations, as these can make your system more vulnerable to malware attacks.

2.2. Computer viruses and their classification

A computer virus is a type of malware that replicates and spreads by attaching itself to legitimate files or software. It is generally refered to programs that unintentionally get into computers, disrupt the normal operation, and cause damage to data and programs. Without the knowledge or consent of the user, it can damage the system and disrupt normal computer operations. They are a common and well-known security threat.

There is no strict classification of computer viruses as technology grows, new and more complex viruses appear every day, which cannot always be assigned to one of the existing categories. Nevertheless, viruses can be classified according to the following characteristics.[10]

2.2.1. Classification based on operating system and environment

- **File Virus**: This type of virus attaches itself to a program. Once activated in the computer's memory, it can infect every program subsequently run on the computer, leading to widespread infection across the system. They have the property of a resident virus. A resident virus inserts its replication module into the host's memory, allowing it to infect other files without needing to be executed. This type of virus is particularly harmful as it can infect the system in several ways, even attaching itself to antivirus software which allows it to infect any file scanned by the programme.
- **Boot Sector Virus**: This virus attacks a computer's master boot record (MBR). It injects its code into the partition table of a hard disk and then moves to the main memory when the computer restarts. Symptoms of this type of virus include boot-up issues, poor system performance, and a hard disk that cannot be located. A boot sector virus can cause booting issues, difficulty finding the hard disk, and poor system performance. However, this type of virus has become less common due to the decline in the use of floppy disks. Many modern computers have built-in boot sector protections that reduce the risk of this virus.
- **Macro Virus**: This virus is written in macro language and runs automatically when a file is opened, and can easily spread to other files. It operates based on the application rather than the operating system. Macro viruses are commonly hidden in files that are often received via emails. Applications like MS Word can allow the embedding of macro viruses in documents.
- **Network Virus**: This virus spreads by using network protocols and email commands.
- **Virus Hoax**: This is an email warning about a nonexistent virus, intended to scare people.

Additionally, there are various combinations of these viruses, such as file-boot or multipartite viruses that infect both files and boot sectors [11]. A multipartite virus uses various techniques to spread across computers. It typically resides in the computer's memory and infects the hard disk, then infects more drives by changing the content of applications. This can cause a decline in performance and low application memory. To avoid multipartite viruses, one should avoid opening attachments from untrusted sources, use reputable antivirus software, and clean the boot sector and the entire disk of the computer. This virus infects and spreads in numerous manners, depending on the operating system of your computer. Another example is the network macro-virus, which not only infects documents being edited but also sends copies of itself via email.

2.2.2. Classification based on operating algorithms

According to their operating algorithms, viruses can be further divided into:

- **TSR (Terminate and Stay Resident) Virus**: This virus leaves a resident part in RAM while infecting a computer. It intercepts system calls to target objects and incorporates itself into them. Resident viruses remain active in memory until the computer is powered down or the operating system is rebooted. Nonresident viruses do not infect computer memory and are only active for a limited time.
- **Stealth Virus**: This virus tries to hide from both the operating system and antivirus software. It resides in the computer’s RAM, actively monitoring the operating system. When performing malicious actions, such as deleting files, it tricks the operating system into thinking everything is normal by hiding signs of its presence.
- **Polymorphic Virus**: This virus uses different algorithms and encryption keys each time it infects an application or programmeme or creates a copy of itself. This makes it difficult for antivirus programmemes to detect, as the virus is constantly changing its encryption. This type of virus is also self-encrypted, adding an additional layer of difficulty for detection.

2.2.3. Classification based on impact

Viruses can be categorized by their level of impact as follows [12]:

- **Low Risk**: These viruses have minimal effect on computer operations. They do not interfere with the computer's functionality but occupy some memory space as they replicate. These viruses might display graphics, messages, simulate sounds, and reduce available disk space.

- **Moderate Risk**: These viruses can significantly disrupt computer operations. Their destructive capabilities vary widely, often damaging or altering executable programs by inserting code at the beginning, disrupting the original byte sequence. Under certain conditions, they might manage disk operations, such as formatting the zero track, thereby destroying crucial information stored on the disk.

- **High Risk**: These viruses cause severe disruptions, potentially leading to the loss of programs and data. They can delete critical system information stored in memory areas necessary for the normal operation of the computer, leading to a complete failure of the system.

2.3. Methods for searching for computer threats

There are several methods that can be followed to search for computer threats [12]:

- **Antivirus Software**: This software uses a database of known threats to scan your computer for malicious files or software. It can also detect and remove any threats that it finds.

- **Malware Scanning**: This is a process of running specialised software to detect and remove malware from your computer. This can include using online scanners, standalone malware scanners, or using a specialised tool built into your operating system.

- **Network Traffic Analysis**: This method involves monitoring and analysing network traffic to detect suspicious or malicious activity. This can include monitoring for unusual traffic patterns, monitoring for known malicious IP addresses, or using specialised software to analyse traffic.

- **File Integrity Monitoring**: This method involves monitoring changes made to files and directories on your computer to detect unauthorised changes. This can help detect malware that modifies files on your system, such as rootkits.

- **Security Log Review**: This method involves reviewing the system and security logs to detect suspicious activity. This can include monitoring failed login attempts, detecting unusual network connections, or monitoring suspicious system events.

- **Vulnerability Scanning**: This method involves identifying known vulnerabilities in software and systems and then checking for those vulnerabilities on your computer.

Specialized antivirus measures include both hardware and software solutions:

- **Hardware Antivirus**: These are specialized antivirus microchips that assume control during the initial system boot, before the system hard disk and OS load. They also scan each drive sector upon access.

- **Antivirus Software**: This is the most commonly used antivirus tool, comprising a system of specialized programs designed to detect and combat viruses.

It is important to keep in mind that no single method is foolproof, and a combination of these methods can provide a more comprehensive protection. Our study will be based on Antivirus softwares.

2.4. Operation of antivirus programmes

Antivirus programmes can be classified into three categories based on their detection method: signature-based, behaviour-based, and machine learning. Another way to categorise antivirus programmes is by the type of operating system they protect, such as Windows, Mac, or Linux.

Antivirus software that uses signature-based detection compares the files on your computer with a database of known malware signatures. These signatures are unique patterns or characteristics that are specific to a particular type of malware. When a match is found between a file on your computer and a known malware signature in the database, the antivirus software will flag the file as potentially malicious and take appropriate action to remove or quarantine the file. Signature-based detection is considered a traditional method of malware

detection and is still widely used today. It is relatively straightforward and easy to implement, but it can only detect malware that is already known, and that is why it is not as effective against new or unknown malware [13].

Behaviour-based antivirus software monitors the actions and activities of programmes and applications on your computer in real-time, looking for any signs of suspicious or malicious behaviour that may indicate the presence of malware. It can detect when an application is trying to access sensitive information or make unauthorised changes to your computer, for example. This method of detection is more effective against new or unknown malware as it detects malware based on its behaviour patterns, rather than relying on a preexisting database of known malware signatures, like signature-based detection. However, behaviour-based detection can also produce more false positives and require more system resources to run.

Machine learning-based antivirus software is a relatively new approach to malware detection. It uses advanced algorithms and techniques from the field of artificial intelligence to analyse and identify malware. This method of detection is based on training machine learning models on large sets of data, including both known well and known bad files. Once the model is trained, it can be used to classify new files as good or bad.

One of the advantages of machine learning-based antivirus software is that it can detect unknown or previously unseen malware by identifying patterns and anomalies that are indicative of malware. It can also learn and adapt to new threats over time. Additionally, it can reduce false positives and improve the overall accuracy of malware detection. However, it requires large amounts of data, which can be difficult to obtain, and it also requires powerful computational resources to run.

The principles of operation of antivirus programmes typically include the following:

- **File Scanner**: This is the process of scanning files on the computer to detect any known or unknown malware. The scan can be done in real-time, on-demand, or scheduled.

- **Signature Matching**: This is the process of comparing the files on the computer to a database of known malware signatures. Any files that match known malware signatures are flagged as potentially malicious.

- **Behaviour Analysis**: This is the process of monitoring the behaviour of programmes and applications running to detect suspicious or malicious activities.

- **Heuristic analysis**: This is the process of using heuristics, or rules of thumb, to detect new or unknown malware that has not been seen before.

- **Quarantine and Removal**: Once malware is detected, it is typically quarantined or removed from the computer to prevent further damage.

- **Automatic Updates**: Antivirus software must be updated regularly to keep its database of malware signatures and threat intelligence up-to-date.

- **Real-time Protection**: Some antivirus software include a feature that can detect and prevent the execution of malware in real time.

- **Cloud-based Protection**: Some antivirus software uses cloud-based technologies to detect and stop malware in real-time.

- **Scheduler**: This component allows the user to schedule scans to run automatically at specific times.

- **Firewall**: This is a security system that monitors and controls incoming and outgoing network traffic and can prevent unauthorised access to a computer or network.

- **Sandboxing**: This is a feature that allows the antivirus software to run a programme or application in a secure environment and monitor its behaviour to detect malicious activities.

It is important to remember that different antivirus software has different features and may use different methods to detect and remove malware.

2.5. Pecularities of antivirus programmes

There are several peculiarities of antivirus programmes that are worth noting [13]:

- **False Positives**: Antivirus software can sometimes flag legitimate files as malicious, which is known as a false positive. This can happen if the software's malware signature database is out of date or if the software is not configured correctly.

- **False Negatives**: Antivirus software can also fail to detect malware, known as a false negative. This can happen if the malware is new or unknown and is not included in the software's database of known malware signatures.

- **Performance Impact**: Some antivirus software can have a significant impact on computer performance, especially when running scans or protecting in real time.

- **Security Alerts**: Some antivirus software can generate a large number of security alerts, which can be overwhelming for users.

- **Compatibility Issues**: Some antivirus software may not be compatible with all operating systems or hardware configurations.

- **Subscription-based**: Many antivirus software are subscription-based, meaning users have to pay for access to the software and updates after a certain period of time.

- **Limited Protection**: Antivirus software typically only protects against malware and viruses, not against other types of cyber threat, such as phishing, spam, and social engineering.

It is important to be aware of these peculiarities when choosing an antivirus program, and to keep in mind that no single software can provide 100% protection against all types of malware or cyber threats.

2.5.1. Preventive Measures

Preventive actions are critical in reducing the risk of virus infections and mitigating potential damage. Key preventive measures include:

- **Write Protection**: Use write-protected media for read-only information.

- **Logical Drive Protection**: Create a write-protected logical drive on the hard drive for data that is used frequently but not altered.

- **Antivirus Scanning**: Scan all applications and files downloaded from the Internet or received through other means before installation. This includes newly acquired software, even if it is licensed.

- **User Restriction**: Limit the number of users on a computer to minimize the risk of unsupervised activity.

- **Regular Updates**: Frequently update antivirus programs to ensure they can detect and counter the latest threats.

Despite these comprehensive measures, it is important to note that no system can be entirely immune to viruses. Constant vigilance and regular updates are essential in maintaining robust protection against evolving threats [13].

3. LITERATURE REVIEW

The inclusion of antivirus software is crucial in protecting personal computers from advancing cyber threats. Nevertheless, there are ongoing apprehensions about its possible influence on system efficiency. This expanded literature review seeks to explore further existing research and analyses to thoroughly grasp the repercussions of antivirus software on personal computer performance, integrating additional factual information and statistical evidence whenever feasible.

The exploration of antivirus software has attracted considerable attention from researchers due to the rising instances of cybercrime worldwide. In [14], the effectiveness and defensive capabilities of antivirus software were analyzed. The study involved testing various antivirus programs against infected Uniform Resource Locators (URLs) containing malware. Forty different antivirus software were employed to evaluate their strength in combating malware threats.

Similarly, [15] conducted a comparative study on the performance of different antivirus software. The authors subjected 193 malicious URLs, linked to malware downloads, to analysis. The findings revealed that many infected URLs failed to compromise selected computer systems and applications, primarily due to regular system patching. This suggests that vulnerabilities present in third-party software applications may have been addressed through patches, rendering them incapable of delivering malicious payloads.

In a contrasting approach, [16] investigated the performance of selected antivirus software, including McAfee, Avast, Avira, Bitdefender, and Norton. The focus of the study was on scanning efficiency, with performance metrics such as full scan, custom scan, and quick scan evaluated. Bitdefender emerged as the top performer among the antivirus solutions tested.

Furthermore, [17] conducted a comparative study on 14 antivirus programs to identify the best antivirus software in 2019. The evaluation involved testing with 432 live malware samples over a period of 700 hours. Bitdefender was found to be the most effective antivirus software based on various parameters, including its impact on computer system performance, malware protection capability, browsing security, and spam filtering effectiveness.

3.1. Antivirus software and system performance

Numerous studies have scrutinized the performance impact of antivirus software, with a focus on various metrics including system boot time, application launch time, and overall system responsiveness.

- **System Boot Time**: A comprehensive analysis by [18] revealed that antivirus software installation can increase system boot time by an average of 20% to 30%, depending on the specific solution deployed.
- **Application Launch Time**: Research conducted by [19] indicated that some antivirus programs can prolong application launch times by up to 50%, significantly impacting user experience and productivity.
- **Overall System Responsiveness**: Benchmark tests conducted by [20] illustrated that while modern antivirus solutions strive for minimal performance degradation, certain operations such as full system scans can lead to a noticeable slowdown, with some programs exhibiting a performance decrease of up to 40%.

3.2. Resource utilization

Studies examining CPU and memory usage shed light on the resource impact of antivirus software on personal computers.

- **CPU Usage**: Findings from [21] demonstrated that antivirus programs can consume a substantial portion of CPU resources, with real-time scanning and system updates often leading to spikes in CPU usage ranging from 20% to 50%.
- **Memory Usage**: Research conducted by [22] highlighted significant variations in memory usage among different antivirus solutions, with some programs utilizing upwards of 500 MB of RAM, potentially affecting multitasking capabilities and overall system performance.

3.3. User experience and perception

Understanding user perceptions and experiences with antivirus software is crucial for assessing its real-world impact.

- **User Perception**: A survey conducted by [23] indicated that while users recognize the importance of antivirus protection, many express frustrations over perceived slowdowns in system performance, with 70% of respondents citing antivirus software as a contributing factor.

- **Usability Studies**: Analysis by [24] emphasized the significance of user-friendly interfaces and efficient background operation in mitigating user dissatisfaction, with studies showing that intuitive antivirus solutions can lead to a 20% improvement in user satisfaction ratings.

3.4. Advancements in antivirus technology

Recent advancements in antivirus technology aim to address performance concerns while maintaining robust security measures.

1. **Cloud-Based Scanning**: Research by [25] highlighted the benefits of cloud-based scanning in offloading processing tasks to remote servers, thereby reducing the performance impact on local machines by up to 60%.

2. **Behavioral Detection**: Innovations in behavioral detection techniques, as discussed by [26] enable antivirus software to monitor application behavior in real-time, minimizing the need for resource-intensive scanning operations and optimizing system performance.

3. **Optimization Techniques**: Examination of optimization techniques by [27] showcased the effectiveness of intelligent caching and incremental updates in reducing performance overhead, with studies reporting a 30% decrease in resource utilization compared to traditional antivirus approaches.

4. RESEARCH METHODOLOGY

4.1. Survey research

Survey research is a widely utilized quantitative research approach employed to gather data from a specific group of participants. Over the years, it has become one of the most prevalent methodologies in various industries, primarily due to its numerous advantages and benefits in data collection and analysis.

Survey Research is defined as the process of conducting research using surveys that researchers send to survey respondents. The data collected from surveys is then statistically analyzed to draw meaningful research conclusions.

Researchers have the flexibility to employ various research methods, but surveys have emerged as a highly effective and reliable approach. Online surveys, specifically, are utilized to gather information on important business topics from individuals or groups. These surveys consist of well-structured questions designed to encourage participants to provide their responses.

Conducting surveys or polls is often the initial step in obtaining prompt information on popular topics, while more comprehensive quantitative research methods or qualitative approaches like focus groups or interviews can be pursued thereafter. Researchers often employ a combination of qualitative and quantitative strategies in various scenarios to conduct their research effectively [28].

Overall, surveys may have following steps :

- **Population and Sample**: The population refers to the entire group of individuals that the survey aims to represent or study. Due to practical constraints, it is often not feasible to survey the entire population. Instead, a sample is selected—a smaller subset of the population that is representative of the larger group. The sample should be carefully chosen to ensure it accurately reflects the characteristics of the population.
- **Survey Instrument**: The survey instrument is the tool used to collect data from the respondents. It typically consists of a set of questions or items designed to gather the desired

information. The instrument can be in the form of a paper questionnaire, an online survey, or a structured interview.

- **Question Design**: Survey questions should be carefully crafted to ensure clarity, avoid bias, and elicit the desired information. Different question types, such as multiple-choice, Likert scale, open-ended, or ranking questions, can be used to gather various types of data. Well-designed questions help ensure accurate and meaningful responses from the participants.
- **Sampling Methodology**: The sampling methodology outlines the process of selecting participants from the population. Various sampling techniques can be used, such as random sampling, stratified sampling, or convenience sampling. The choice of sampling method depends on the research objectives and available resources.
- **Data Collection**: Surveys can be administered through various methods, including online surveys, face-to-face interviews, telephone interviews, or mailed questionnaires. The chosen method should be appropriate for the target population and research goals. Data collection involves distributing the survey, collecting responses, and ensuring data accuracy and integrity.
- **Data Analysis**: Once the survey responses are collected, data analysis techniques are applied to derive meaningful insights. This may involve quantitative analysis, such as statistical calculations and interpretation, or qualitative analysis, which focuses on themes and patterns within open-ended responses. The goal is to uncover trends, relationships, and findings that address the research objectives.
- **Reporting and Interpretation**: The final step involves summarizing the survey findings in a comprehensive report. This report should include a clear interpretation of the results, highlighting key findings, trends, and implications. Effective communication of the survey results ensures that the collected data is utilized for decision-making, research, or further investigation.

Survey research methods can be categorized based on two key factors: the survey research tool used and the time required to conduct the research.

There are three primary survey research methods, classified according to the medium of data collection:

- **Online/Email**: Online surveys have gained significant popularity as a cost-effective and accurate method. They require minimal investment and yield highly precise responses.
- **Phone**: Phone surveys, known as Computer-Assisted Telephone Interview (CATI) surveys, allow researchers to collect data from a broader segment of the target population. While they may involve higher costs and more time compared to other methods, they can be effective in gathering information.
- **Face-to-face**: Face-to-face surveys, often conducted through in-depth interviews, are suitable for complex problem-solving situations. This method tends to have the highest response rate, but it can be costly.

Additionally, survey research can be classified based on the time frame involved:

- **Longitudinal survey research**: This method involves conducting surveys over an extended period, spanning years or even decades. Researchers collect qualitative or quantitative data at different time intervals to observe changes in respondent behavior, preferences, and attitudes over time. Longitudinal studies provide insights into reasons behind these changes. For example, a researcher studying teenagers' eating habits may follow a sample of teenagers over a considerable period to analyze reliable information. Cross-sectional surveys are often conducted alongside longitudinal studies.

- **Cross-sectional survey research**: Cross-sectional surveys gather data from a target audience at a specific time interval. They are commonly used in various sectors such as retail, education, healthcare, and small-to-medium-sized enterprises (SMEs). Cross-sectional studies can be either descriptive or analytical and allow researchers to quickly collect information within a brief period. This method is useful when a descriptive analysis of a subject is required.

In our study, we have conducted a survey to around 130 students out of which it got 75 responses. The goal of the survey is to highlight the most popular free and paid antivirus programs.

Survey Topic: Impact of Antivirus on PC Performance: A Survey.

Target Audience: Students

Responses: 75

Survey Platform: Google forms

Survey Link:

https://docs.google.com/forms/d/e/1FAIpQLSebQUS5atpxeHyc1KoX470wctNSTuNBxI6-lmKVVkA5Fw6T0Q/viewform?usp=sf_link

Here are some popular survey tools that were considered for conducting surveys:

- SurveyMonkey
- Google Forms
- Qualtrics
- Typeform
- Microsoft Forms
- SurveyGizmo
- Poll Everywhere
- SurveyLegend

These are just a few examples, and there are many more survey tools available in the market. In this survey, Google Forms is preferred since it is a smaller-scale survey with around 100 people. Several advantages are considered:

Simplicity and User-Friendliness: Google Forms has a straightforward and intuitive interface, making it easy for both survey creators and respondents to use. It requires no coding skills and provides a simple drag-and-drop interface for question creation.

Cost-Effective: Google Forms is free to use, which makes it a cost-effective choice, especially for smaller projects with limited budgets.

Seamless Integration: Since Google Forms is a part of the Google Suite, it seamlessly integrates with other Google applications, such as Google Sheets for data collection and analysis. This integration simplifies the process of collecting and managing survey responses.

Collaborative Features: Google Forms allows multiple users to collaborate on survey creation and data analysis in real-time.

Response Collection and Analysis: Google Forms automatically collects and compiles survey responses in a Google Sheets spreadsheet. This makes it convenient to manage and analyze the data within a familiar and widely-used platform.

Customizable and Versatile: Google Forms offers various question types, including multiple-choice, dropdowns, checkboxes, and open-ended questions. It also allows you to customize the survey's appearance, branding, and layout.

Accessibility: Google Forms can be accessed and completed on various devices, including desktop computers, laptops, tablets, and smartphones. This ensures flexibility for respondents to participate at their convenience.

Questionnaire and Responses:

A total of 12 questions were included in the survey. The questions were designed with visuals to make it interesting to the audience.

These questions were useful in understanding the antivirus popularity based on user experience.

Figure 1 shows the response for question “How often do you use antivirus software on your personal computer?“. 35.1% of users rarely use antivirus software. Many users have added comments with the reason that it’s a hassle and nusense on the computer.

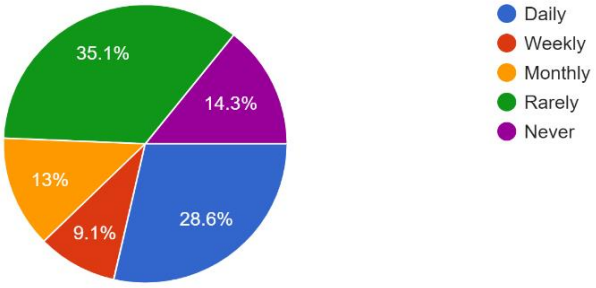

Fig. 1 Frequency of antivirus usage by respondents

Figure 2 shows that most people like to use free antivirus. Also some part do not like to use any antivirus at all. Response to the question “What type of antivirus software do you currently use?“

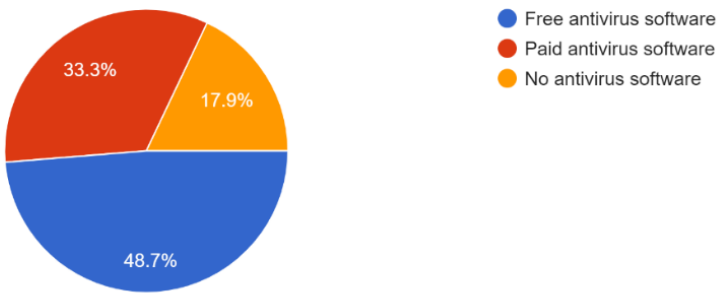

Fig. 2 Type of antivirus software most respondents use

When asked Would you be willing to pay for an antivirus program?, Figure 3 shows that most people would not like to pay for the antivirus given a choice.

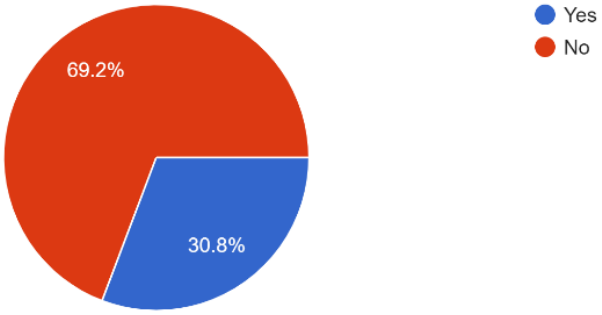

Fig. 3 Willingness to pay for an antivirus program

Figures 4 and 5 show the response for free and paid antivirus respectively. The majority have chosen Windows Defender in free antivirus and it even shows in Figure 5 that most people would like to choose free antivirus.

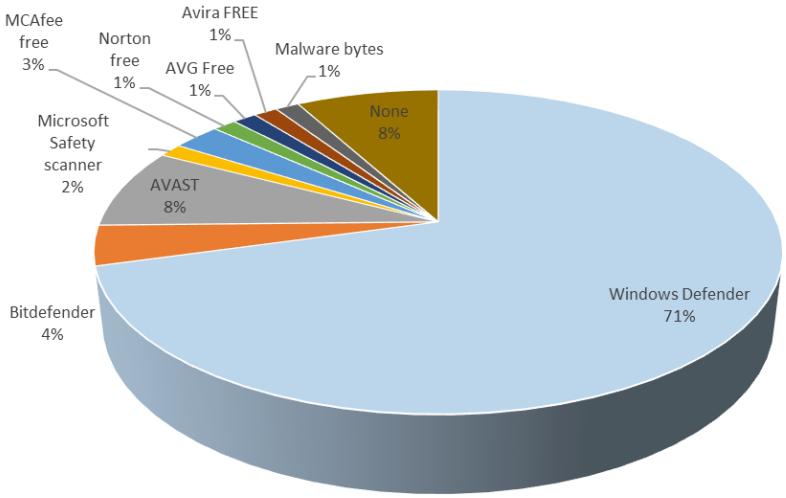

Fig. 4 Survey results: selection of free antivirus for testing

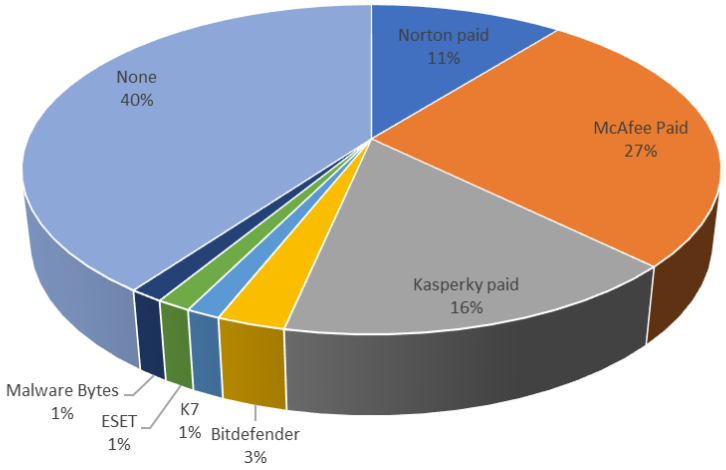

Fig. 5 Survey results: selection of paid antivirus for testing

Based on the survey results 6 antivirus programs were selected for the study: 3 free antivirus programs and 3 paid.

Free antivirus programs:

- Windows Defender.
- Bitfender Free.
- Avast Free.

Paid antivirus programs:

- Norton 360 Antivirus.
- McAfee (McAfee® Total Protection™ - Essential).
- Kaspersky (Kaspersky Standard).

4.2. The testing process

The algorithm of the testing process is presented in Figure 6.

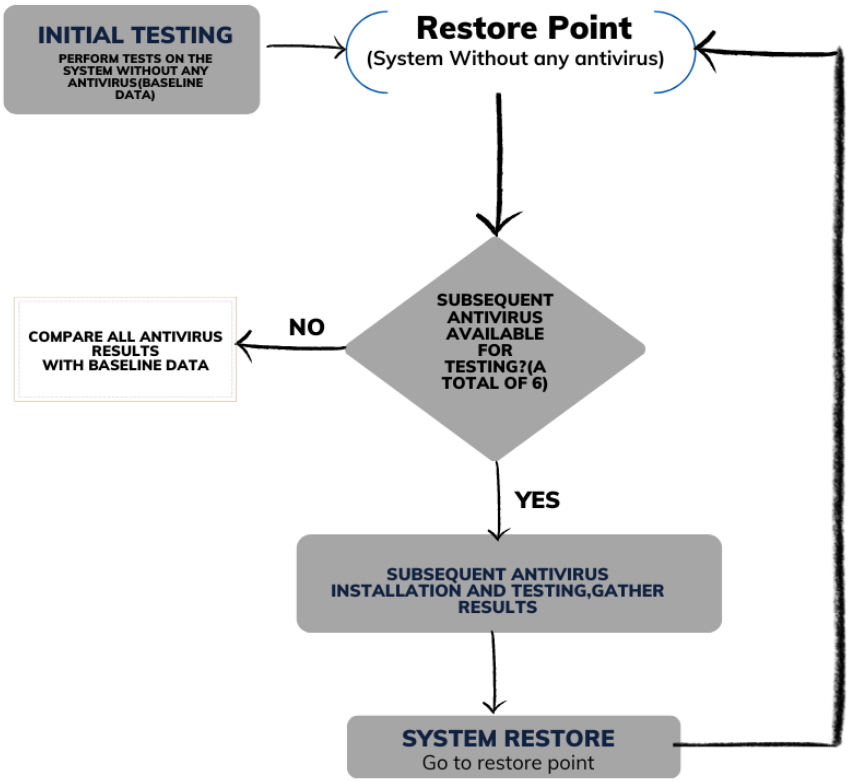

Fig. 6 The testing process

The testing process is carried out in several steps:

Initial testing: initiate testing without the presence of any antivirus software.

Create restore point: before proceeding with antivirus installation, create a restore point using the operating system recovery tool. This will serve as a baseline for comparison and system restoration if necessary.

Antivirus installation: install the antivirus program under investigation and conduct corresponding tests. Tests performed:

1. Working memory used by antivirus programs.

2. The impact of antivirus programs on personal computer start-up.

3. The impact of antivirus programs on the process of various application start-up.

4. The impact of antivirus programs on the process of copying set of files.

System restore: system restores upon completing assessments for the first antivirus in the operating system, restore system settings to the pre-antivirus installation state using the operating system recovery tool, specifically “System Recovery - Reset this PC”

Subsequent antivirus installation: install another antivirus program, maintaining consistency in operating system settings and the array of installed programs for a standardized testing environment. This approach ensures a systematic and fair evaluation of each antivirus, allowing for accurate comparisons based on identical operating conditions.

Note: The testing was done with the same personal computer: unchanged hardware specification and same programs/applications installed before and during testing.

4.3. Experimental Environment

OS Name:	Microsoft Windows 10 Pro
OS Version:	10.0.19045 N/A Build 19045
OS Manufacturer:	Microsoft Corporation
OS Configuration:	Standalone Workstation
OS Build Type:	Multiprocessor Free
System Manufacturer:	Dell Inc.
System Model:	Latitude E7440
System Type:	x64-based PC
Processor(s):	Intel64 Family 6 Model 69 Stepping 1 GenuineIntel ~2000 Mhz

BIOS Version: Dell Inc. A28, 13-06-2019

RAM: 8 GB

Disk Drive type: Solid State Drive

4.4. Software used for testing

PassMark AppTimer: AppTimer, developed by PassMark Software, is a tool designed for benchmarking an application's startup time (Fig. 7). It accomplishes this by executing a given application multiple times, measuring the duration it takes for the application to reach a state where user input is accepted, and then automatically closing the application. The startup time measurements are logged to a file. AppTimer is a free utility.

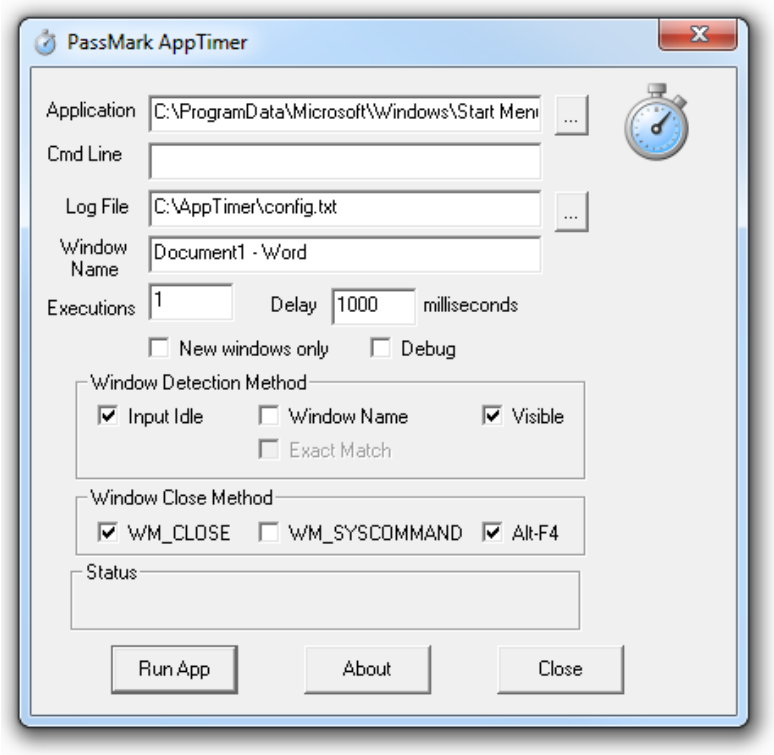

Fig. 7 PassMark Apptimer

This tool proves valuable in performance testing scenarios where one needs to compare the startup times of different applications on the same hardware or evaluate the impact of varying hardware configurations on the startup time of a specific application. AppTimer ensures consistent and repeatable measurements, particularly beneficial when the startup time of

applications is relatively short, making manual measurements with a stopwatch less reliable (AppTimer, 2024).

BootRacer: BootRacer is a lightweight, user-friendly, and convenient tool designed for monitoring the boot time of Windows PCs and managing startup programs (Fig. 8.). BootRacer stands out with its ability to exclude the user password timeout time from the overall calculated boot time, providing a more accurate measurement. BootRacer calculates the clear Windows boot-up time (without password timeout).

Fig. 8 BootRacer

Windows PowerShell: PowerShell is a task automation framework and scripting language developed by Microsoft (Fig. 9). It is specifically designed for system administration, configuration management, and automation of repetitive tasks. PowerShell is built on the .NET Framework and supports the automation of administrative tasks via cmdlets (pronounced "command-lets"), which are specialized .NET classes (PowerShell, 2024).

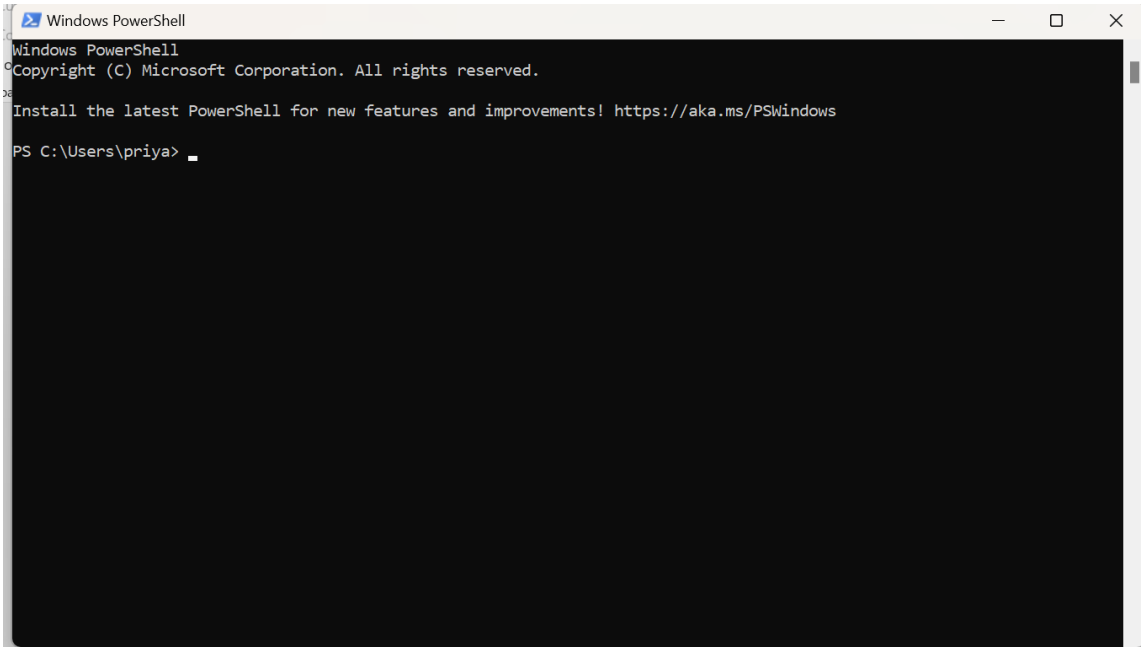

Fig. 9 Windows PowerShell

5. Experimental results: impact of various antiviruses on personal computer performance

These are the average results of experiments with 10 iterations.

Note: The results are in comparison to the computer performance when no antivirus program is installed (as a baseline).

5.1. Working memory used by antivirus programs

The working memory of a process refers to the temporary storage and manipulation of data that is actively being used or processed by the specific task or program. It is a crucial aspect of a computer's memory system and is distinct from long-term storage, as it is designed to hold information that is immediately required for ongoing computations or operations. PowerShell is used here. Computer random access memory usage by various antivirus programs working set is shown in Figure 10.

Fig. 10 Memory usage by various antivirus programs working set

In the assessment of working memory utilization by various antivirus processes, Windows Defender registers the highest consumption at 240.38 MB, indicative of its comprehensive security features. Bitdefender Free exhibits a more frugal impact, utilizing 35.06 MB of memory, presenting a lightweight yet effective alternative. Avast Free strikes a balance, using 68.06 MB, offering a moderate footprint with robust protection. Norton 360 and

McAfee Total Protection showcase higher memory utilization at 196.74 MB and 219.9 MB, respectively, emphasizing their feature-rich security suites. Kaspersky Standard stands out with the lowest memory footprint at 18.28 MB, highlighting its efficiency in delivering security with minimal impact on system resources. These results underscore the diverse trade-offs users must consider when selecting an antivirus solution based on their preferences for both security features and system performance.

5.2. The impact of antivirus programs on personal computer start-up

The installation of an antivirus program on a computer typically leads to an increase in both the startup time and the operating system boot time. Considering a program's impact on computer bootup is crucial for optimizing system performance and user experience. Slow boot times can frustrate users and hinder productivity, while inefficient programs may consume valuable system resources. Managing startup processes effectively ensures quicker boot times and improved stability for the system. This segment presents the findings from studies examining the influence of antivirus programs on startup time. Each antivirus program underwent 10 experiments, comparing its impact on computer startup time to scenarios where it was entirely absent from the system. To test the Bootup duration, BootRacer Application is used.

Figure 11 contains the averages of the results of 10 experiments, when the computer was started with or without a certain antivirus program installed.

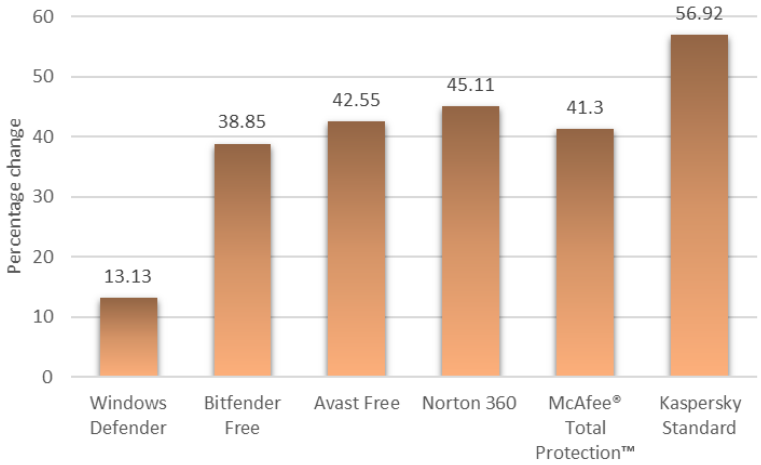

Fig. 11 Change in computer boot-up duration

In the investigation of antivirus impact on boot duration, Windows Defender, as the native option, introduces a moderate increase by 13.13% compared to system with no antivirus, demonstrating a balanced compromise between security and performance. Moving to third-party solutions, Bitdefender Free and Avast Free exhibit moderate impacts with less than 50% increase. Paid antiviruses Norton 360 and McAfee Total Protection present moderate impacts, emphasizing the trade-off between robust security features and startup speed. Kaspersky Standard, with the longest boot time which is ~57% more than the baseline, indicates a higher impact on system startup, underscoring the advanced security measures provided. The findings suggest that users must weigh their preferences for enhanced security against the associated impact on startup performance when selecting an antivirus solution.

5.3. The impact of antivirus programs on the process of various application start-up

The impact of antivirus programs on application launch was investigated in this study. Users frequently utilize various applications during computer tasks, prompting an experimental examination of how antivirus programs affect application initiation. The study focused on four widely used applications: Microsoft Office Word 2016, Microsoft Powerpoint 2016, Microsoft Edge, and Notepad. Each application was subjected to testing both with and without various antivirus programs installed on the computer. The AppTimer program facilitated launching each application ten times, allowing for the measurement of the time taken for application initiation in each scenario (Fig. 12).

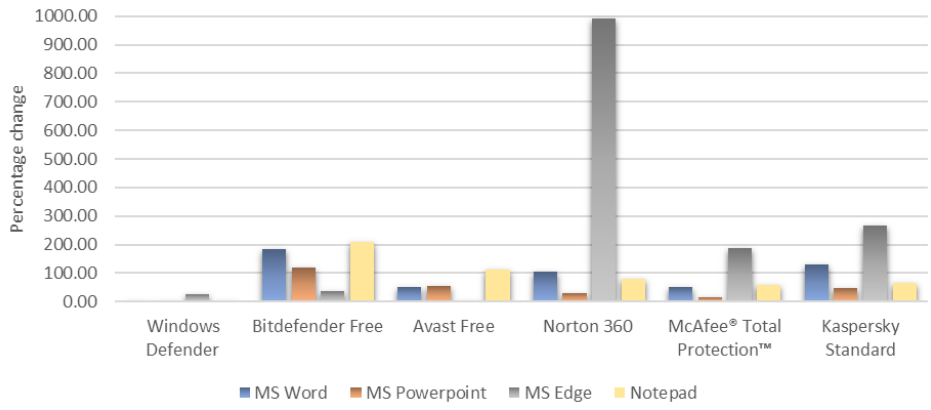

Fig. 12 Change in application start-up duration

In summary, the application startup times for various antivirus solutions reveal distinct performance impacts. Windows defender showed very less impact on various application start-up time, almost similar compared to a system with no antivirus. In Figure 12, the start-up time for Microsoft Edge is around 28 % more with Windows defender, whereas Norton 360 antivirus shows a very high start-up time for Microsoft Edge. Windows Defender caches the application files, and is seamlessly integrated with the operating system. It boosts security and streamlines application management for users. Avast Free also starts up Microsoft Edge quite quickly with browser control cache. Windows Defender emerges as the most efficient, significantly reducing initiation times across all applications. Bitdefender Free shows increased startup times, particularly in MS Word. Avast Free strikes a balance with moderate startup times. Norton 360 introduces notable delays in MS Edge, potentially affecting web browsing. McAfee Total Protection demonstrates competitive and balanced startup times. Kaspersky Standard exhibits moderate initiation times across applications. Choosing an antivirus solution should consider these trade-offs between security features and application performance based on user priorities.

5.4. The impact of antivirus programs on the process of copying set of files

A prevalent user activity on computers is the copying of files. Hence, the objective of this study is to assess the impact of antivirus software on the speed of the file copying process. The study involves copying a set of files, varying in size and format, from one logical drive to another on a computer. Powershell Script is run to copy files and get the time taken by the operation.

The combined size of the file set (Fig. 13, 14) is 3.28 GB, comprising a total of 15707 files and 2954 folders. This set contains various file types, and the folders that also contains archives that store multiple files, such as *.exe, *.zip, *.rar and others.

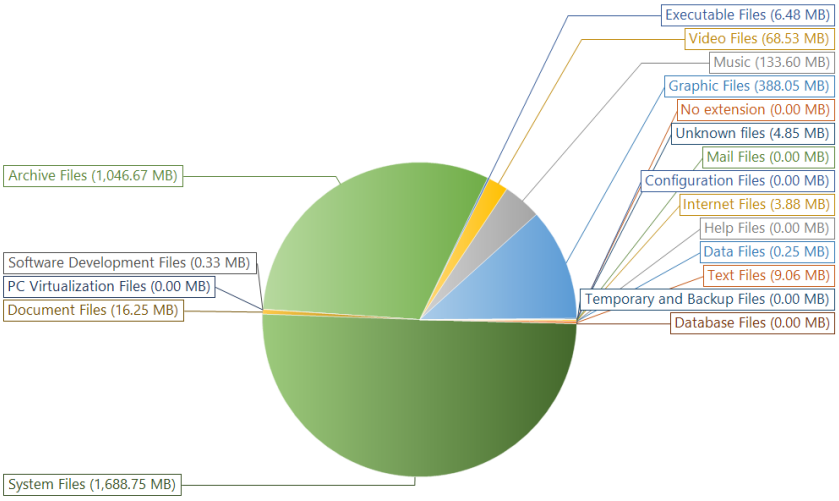

Fig. 13 Groups of file types by size in a set

Type	Ext
7Z File	.7z
BIN File	.bin
DS_STORE File	.DS_Store
FLV File	.flv
GITATTRIBUTES File	.gitattributes
GITMODULES File	.gitmodules
Microsoft Edge HTML Document	.MHT
MP3 File	.mp3
MP4 File	.mp4
MXF File	.mxf
OpenDocument Presentation	.odp
PBXPROJ File	.pbxproj
PODSPEC File	.podspec
Microsoft PowerPoint 97-2003 Presentation	.ppt
RAR File	.rar
SWIFT-VERSION File	.swift-version
TIFF File	.tiff
VOB File	.vob
WAV File	.wav
XCWORKSPACEDATA File	.xcworkspacedata
Microsoft Excel Worksheet	.xlsx
Microsoft Edge HTML Document	.xml
Microsoft Excel Worksheet	.xlsx
Microsoft Edge HTML Document	.xml
Application	.exe
Configuration settings	.ini
PROTO File	.proto
SH File	.sh
Microsoft Excel Comma Separated Values File	.csv
PLIST File	.pliist
XCSCHEME File	.xcscheme
Compressed (zipped) Folder	.zip
AVI File	.avi
Microsoft Word Document	.docx
GITIGNORE File	.gitignore
SWIFT File	.swift
YML File	.yml
TTX File	.ttx
MKV File	.mkv
JPEG File	.jpeg
GIF File	.GIF
PY File	.py
CATEGORY File	.category
MOV File	.mov
MD File	.md
PNG File	.PNG
Microsoft Edge HTML Document	.svg
YAML File	.yaml
JPG File	.jpg
PB File	.pb
Text Document	.txt
Microsoft Edge HTML Document	.html
TEXTPROTO File	.textproto
TrueType font file	.ttf

Fig. 14 File types in a set

Figure 15 shows the average file set copy times.

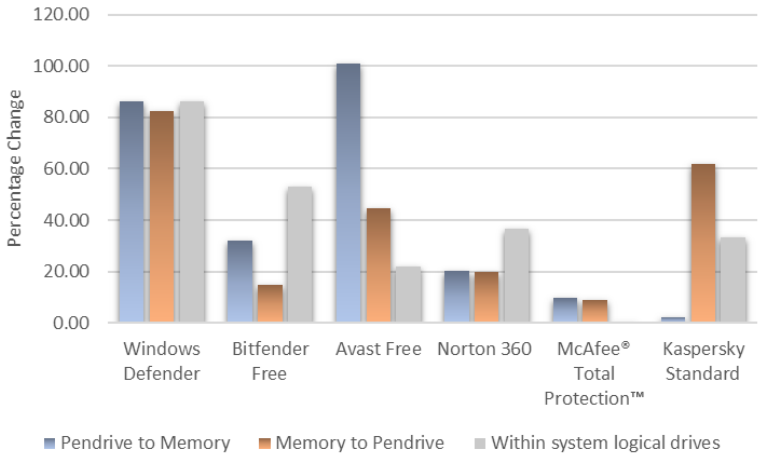

Fig. 15 Change in average file set copy times

In the evaluation of file transfer times across different scenarios, the study considered three aspects: transfers from secondary devices to memory, transfers from memory to secondary devices, and transfers within system logical drives. The results reveal notable variations in the performance of antivirus programs. McAfee showed just approximately 9 % increase in transfers to and from secondary devices and moreover reduced time for internal copying. Windows defender showed an increase of about 80 % for all types of transfers. Avast Free exhibited a comparatively slower file transfer from secondary devices to memory, while Windows Defender and Kaspersky Standard demonstrated extended durations in memory-to-secondary-device transfers. Within system logical drives, Avast Free showed a longer file transfer time, contrasting with McAfee Total Protection, which exhibited a relatively quicker transfer. These findings shed light on the nuanced impacts of antivirus programs on various file transfer scenarios, offering valuable insights for users seeking optimal performance in different contexts.

In summary, the thorough evaluation of various antivirus solutions has yielded nuanced insights into their distinctive impacts on diverse facets of computer performance. Windows Defender emerges as a standout performer, significantly reducing application startup times across the spectrum. Bitdefender Free and Avast Free display moderate startup delays, with Bitdefender particularly influencing the initiation time of MS Word. Notably, Norton 360 introduces substantial delays in the initiation of MS Edge, potentially impacting the overall web

browsing experience. McAfee Total Protection stands out for its competitive and balanced startup times across applications. Meanwhile, Kaspersky Standard demonstrates moderate initiation times in various applications.

CONCLUSIONS AND RECOMMENDATIONS

In summary, the following conclusions can be formulated:

1. Tested antivirus programs can take up to about 240 MB of memory. This can make up a fairly significant percentage of the remaining free random-access memory of the PC.

2. Antivirus programs we tested can slow down a PC's boot time by as much as 57 percent. This highlights the trade-off between security and start-up performance for user consideration.

3. Antivirus program integrated into the operating system showed very less impact on various application start-up time, almost similar compared to a system with no antivirus.

4. The tested paid antivirus programs work particularly poorly with the Microsoft Edge browser, i.e. greatly increases its start-up time.

5. The antivirus solution integrated into the operating system demonstrates an impressive slowdown of about 80 % for all types of data transfers.

6. Thus, when looking for a well-balanced antivirus solution, user should pay attention to antivirus software with efficient resource allocation, start-up time, optimized file transfer speed and relatively lower memory usage.

In conclusion, the findings underscore the significance of considering trade-offs between security features and application performance when selecting an antivirus solution. The individual preferences and priorities of users play a crucial role in determining the most suitable antivirus solution for their specific needs.

References

1. Gandotra, E., Bansal, D., Sofat, S. Malware analysis and classification: a survey. Journal of Information Security, 2014.
2. Barriga, J. J., Yoo, S. G. Malware detection and evasion with machine learning techniques: a survey. International Journal of Applied Engineering Research, 2017, 12(18).
3. Altyeb Altaher, Sureswaran Ramadass, Ammar Ali. Computer Virus Detection Using Features Ranking and Machine Learning. Australian Journal of Basic and Applied Sciences, 2011, 5(9): 1482-1486, ISSN: 1991-8178.
4. Soumen Chakraborty. A Comparison Study of Computer Virus and Detection Techniques. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2017, 2(1). ISSN: 2456-3307.
5. Essam Al Daoud, Iqbal H. Jebril, Belal Zaqaibeh. Computer Virus Strategies and Detection Methods. International Journal of Open Problems in Computer Science and Mathematics, 2008, 1(2).
6. Dogonyaro, N. M., Victor, W. O., Shafii, A. M., Obada, S. L. Comparative Performance Analysis of Anti-virus Software. Information and Communication Technology and Applications, ICTA 2020. Communications in Computer and Information Science, 2021, Vol. 1350. Springer, Cham. https://doi.org/10.1007/978-3-030-69143-1_33.
7. V. Tasril, M. Ginting, M. Mardiana, A. P. U. Siahaan. Threats of computer system and its prevention. International Journal of Scientific Research in Science and Technology, 2017, 3: 448-451.
8. Subramanya, S.R., Lakshminarasimhan, N. Computer viruses. IEEE Potentials, 2001, 20(4): 16-19. DOI: https://doi.org/10.1109/45.969588.
9. Malwarebytes. Signs of Malware. https://www.malwarebytes.com/signs-of-malware/. Accessed 2024-05-24.
10. Pankaj Kumar. Computer Virus Prevention & Antivirus Strategy. Sahara Arts & Management Academy Series. Available at SSRN: https://ssrn.com/abstract=945758 or http://dx.doi.org/10.2139/ssrn.945758.
11. Marc Fossi, et al. Symantec internet security threat report trends for 2010. Volume XVI, 2011.

12. Ahmet Ali Suzen. A risk-assessment of cyber attacks and defense strategies in industry 4.0 ecosystem. International Journal of Computer Network and Information Security, 2020, 14(1).
13. R. Palacios. Evaluation of Local Security Event Management System vs. Standard Antivirus Software. Applied Sciences, 2021, 12(3): 1076. https://doi.org/10.3390/app12031076.
14. E. Willems. The antivirus companies. In: Cyberdanger, Springer, Cham, 2019, pp. 65-83. https://doi.org/10.1007/978-3-030-04531-9_5.
15. A.H. Johar, A. Gerard, N. Athar, U. Asgher. Feature based comparative analysis of online malware scanners (OMS). In: Ayaz, H., Asgher, U. (eds.) AHFE 2020. Advances in Intelligent Systems and Computing, Springer, Cham, 2021, vol. 1201, pp. 385-392. https://doi.org/10.1007/978-3-030-51041-1_51.
16. S. Alqurashi, O. Batarfi. A comparison of malware detection techniques based on hidden Markov model. Journal of Information Security, 2016, 7(3): 215-223.
17. N. Johnston. The best antivirus software for 2018. https://www.toptenreviews.com/software/security/best-antivirus-software/. Accessed 2024-05-24.
18. Symantec Corporation. Impact of Antivirus Software on System Boot Time. Retrieved from Symantec, 2019. Accessed 2024-05-24.
19. AV-Comparatives. Antivirus Software Performance Test. Retrieved from AV-Comparatives, 2020. Accessed 2024-05-24.
20. PassMark Software. Antivirus Performance Benchmark Test. Retrieved from PassMark Software, 2021. Accessed 2024-05-24.
21. Tom's Hardware. CPU Usage and Performance Impact of Antivirus Software. Retrieved from Tom's Hardware, 2018. Accessed 2024-05-24.
22. PCMag. Memory Usage and System Performance: A Comparative Study of Antivirus Programs. Retrieved from PCMag, 2019. Accessed 2024-05-24.
23. Consumer Reports. User Perception and Experience with Antivirus Software. Retrieved from Consumer Reports, 2020. Accessed 2024-05-24.
24. NortonLifeLock. User Satisfaction and Usability of Antivirus Solutions. Retrieved from NortonLifeLock, 2021. Accessed 2024-05-24.

25. Trend Micro. Benefits of Cloud-Based Scanning in Antivirus Software. Retrieved from Trend Micro, 2021. Accessed 2024-05-24.
26. Kaspersky Lab. Behavioral Detection Techniques in Modern Antivirus Software. Retrieved from Kaspersky Lab, 2022. Accessed 2024-05-24.
27. ESET. Optimization Techniques in Antivirus Software Development. Retrieved from ESET, 2020. Accessed 2024-05-24.
28. R.M. Groves, F.J. Fowler, M.P. Couper, J.M. Lepkowski, E. Singer, R. Tourangeau. Survey Methodology. Wiley, 2009. ISBN: 9780470465462. Available at: https://books.google.lt/books?id=HXoSpXvo3s4C.

Appendix A

eStream 2024 Certificate

VILNIUS TECH
Elektronikos fakultetas

8th Open International Conference "Electrical, Electronic and Information Sciences"

eStream 2024

CERTIFICATE

Priyanka Wagle and
Gediminas Gražulevičius

Delivered an Oral Presentation

INVESTIGATION AND EVALUATION OF THE IMPACT OF ANTIVIRUS PROTECTION ON THE PERFORMANCE OF A PERSONAL COMPUTER

Chair of Science Committee Prof. Dr Dalius Navakauskas

Section Chair Assoc. Prof. Dr Dainius Udris

April 25, 2024
Vilnius

APPENDIX B

Publication Acceptance Certificate

KAUNO TECHNIKOS KOLEGIJA

KAUNO TECHNIKOS KOLEGIJA

Viešoji įstaiga, Tvirtovės al. 35, LT-50155 Kaunas, tel. (8 37) 30 86 20, el. p. ktk@edu.ktk.lt.
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 111967869.

Vilniaus Gedimino technikos universitetui – VILNIUS TECH

2024-06-03 Nr.V16-104

DĖL STRAIPSNIO PUBLIKAVIMO

Autorių **Priyanka Wagle, Gediminas Gražulevičius** *(VILNIUS TECH)* straipsnis **Investigation and Evaluation of the Impact of Antivirus Protection on the Performance of a Personal Computer** priimtas publikuoti į mokslinio žurnalo „Inžinerinės ir edukacinės technologijos“ (ISSN 2029-9303) 2024 metų 1 numerį.

Vyr. redaktorė Lina Girdauskienė

Giedrė Adomavičienė, tel. 8 61157620, el. p. giedre.adomaviciene@edu.ktk.lt