Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Engineering

Bachelor Thesis

Antivirus Software in Cyber Security

BATIKAN FALAY

BACHELOR THESIS ASSIGNMENT

Batikan Falay

Informatics

Thesis title

Antivirus Software in Cyber Security

Objectives of thesis

This thesis investigates the field of the antivirus branch in cyber security. The thesis aims to analyze the antivirus programs, and tools in cyber security. The partial objectives of the thesis are:

- to characterize the fundamentals of cybersecurity,
- to identify possibilities of researched and found antivirus programs,
- to compare the found antivirus programs, review of surveys and interviews,
- to evaluate the surveys and interviews found.

Methodology

The methodology of this thesis, thesis will be divided into 2 parts. In the first part, the cyber security will be introduced. Subsequently, the place of antiviruses in cyber security will be mentioned. In the second part of thesis, it will explain what is Antivirus and what it means, and the comparison of the most used antivirus programs in the world, their surveys and interviews with the managers of the antivirus programs found will be evaluated and a score will be made about them.

The proposed extent of the thesis

30 – 40 pages

Keywords

cyber security, cyber risk, antivirus, antivirus software

Recommended information sources

Andreea Bendovschi, Cyber-Attacks – Trends, Patterns and Security Countermeasures, Procedia Economics and Finance, Volume 28, 2015, Pages 24-31, ISSN 2212-5671, https://doi.org/10.1016/S2212-5671(15)01077-1.

Bakhshi, T., Papadaki, M. and Furnell, S. (2009), "Social engineering: assessing vulnerabilities in practice", Information Management & Computer Security, Vol. 17 No. 1, pp. 53-63. https://doi.org/10.1108/09685220910944768

David Tayouri, The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages, Procedia Manufacturing, Volume 3, 2015, Pages 1096-1100, ISSN 2351-9789, https://doi.org/10.1016/j.promfg.2015.07.181.

Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl, Advanced social engineering attacks, Journal of Information Security and Applications, Volume 22, 2015, Pages 113-122, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2014.09.005.

Salahdine, Fatima, and Naima Kaabouch. 2019. "Social Engineering Attacks: A Survey" Future Internet 11, no. 4: 89. https://doi.org/10.3390/fi11040089

Expected date of thesis defence

2021/22 SS – FEM

The Bachelor Thesis Supervisor

doc. Ing. Jan Tyrychtr, Ph.D.

Supervising department

Department of Information Engineering

Electronic approval: 1. 11. 2021
Ing. Martin Pelikán, Ph.D.
Head of department

Electronic approval: 23. 11. 2021
Ing. Martin Pelikán, Ph.D.
Dean

Prague on 24. 02. 2023

Declaration

I declare that I have worked on my bachelor thesis titled "Antivirus Software in Cyber Security" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break any copyrights.

In Prague on 15.03.2023 ______________________________

Acknowledgement

I would like to thank doc. Ing. Jan Tyrychtr, Ph.D for the advice and support he gave me during my work on my thesis.

Antivirus Software in Cyber Security

Abstract

The importance of cybersecurity has increased in recent years due to the growing number of cyber threats and attacks. One critical aspect of cybersecurity is the utilization of antivirus software to detect and remove viruses. This investigation examines the effectiveness of four well-known antivirus programs, namely Kaspersky, Bitdefender, ESET, and McAfee.

The study includes a performance test to assess each program's capability to detect and eliminate viruses. The performance test evaluates the ability of each program to detect a variety of viruses, including known and emerging threats. The outcomes of the performance test demonstrate that all four programs are effective in detecting and eliminating viruses, with Kaspersky and Bitdefender performing better than others.

Furthermore, the study uses Saaty’s Method, also known as the Analytic Hierarchy Process (AHP), to evaluate the programs. The AHP is a decision-making tool that allows for the comparison of various alternatives based on a set of criteria. The evaluation using AHP considers several criteria, including performance, protection, cost, and help & support.

The results of this research have significant implications for both individuals and organizations seeking to improve their cybersecurity measures. The outcomes suggest that investing in high-quality antivirus software programs, such as Kaspersky and Bitdefender, can substantially enhance an organization's ability to detect and remove viruses. Additionally, the study underscores the importance of considering various criteria, including ease of use, price, and customer support, when selecting an antivirus software program. This study provides valuable insights for individuals and organizations looking to enhance their cybersecurity practices.

Keywords: Cyber security, Cyber risk, Antivirus, Antivirus Software, Viruses, Malware

Antivirový software v kybernetické bezpečnosti

Abstrakt

Význam kybernetické bezpečnosti se v posledních letech zvyšuje díky rostoucímu počtu kybernetických hrozeb a útoků. Jedním z kritických aspektů kybernetické bezpečnosti je použití antivirového softwaru k detekci a odstraňování virů. Toto šetření zkoumá účinnost čtyř známých antivirových programů, jmenovitě Kaspersky, Bitdefender, ESET a McAfee.

Studie zahrnuje výkonnostní test k posouzení schopnosti každého programu detekovat a eliminovat viry. Test výkonu hodnotí schopnost každého programu detekovat různé viry, včetně známých a nově vznikajících hrozeb. Výsledky testu výkonu ukazují, že všechny čtyři programy jsou účinné při detekci a odstraňování virů, přičemž Kaspersky a Bitdefender si vedou lépe než ostatní.

Kromě toho studie používá k hodnocení programů Saatyho metodu, známou také jako proces analytické hierarchie (AHP). AHP je rozhodovací nástroj, který umožňuje srovnání různých alternativ na základě souboru kritérií. Hodnocení pomocí AHP bere v úvahu několik kritérií, včetně výkonu, ochrany, nákladů a pomoci a podpory.

Výsledky tohoto výzkumu mají významné důsledky pro jednotlivce i organizace, které se snaží zlepšit svá opatření v oblasti kybernetické bezpečnosti. Výsledky naznačují, že investice do vysoce kvalitních antivirových softwarových programů, jako jsou Kaspersky a Bitdefender, mohou podstatně zlepšit schopnost organizace detekovat a odstraňovat viry. Studie navíc zdůrazňuje, že při výběru antivirového softwaru je důležité zvážit různá kritéria, včetně snadnosti použití, ceny a zákaznické podpory. Tato studie poskytuje cenné poznatky jednotlivcům a organizacím, které chtějí zlepšit své postupy v oblasti kybernetické bezpečnosti.

Klíčová slova: Kybernetická bezpečnost, Kybernetická rizika, Antivirus, Antivirový software, Viry, Malware

Table of content

List of figure

List of Tables

List of Abbreviations

DDoS	Denial-of-service
PAS	CyberArk Privileged Access Security Solution
IDS	Intrusion detection systems
APTs	Advanced persistent threats
MITM	Man-in-the-middle
AHP	Analytic hierarchy process
SD	Secure Digital
USB	Universal Serial Bus
ACD	Automatic Call Distribution
CI	Consistency Index
RI	Random Consistency Index

1 Introduction

As technology advances, cybersecurity has become a growing concern for individuals and organizations alike. The number of cyberattacks is increasing at an alarming rate, and their consequences can be severe, ranging from data breaches and financial losses to reputational damage and even national security threats. One of the essential tools in combating cyber threats is antivirus software, which is designed to prevent, detect, and remove malicious software from computer systems.

While there are numerous antivirus software programs available on the market, the effectiveness of each program can vary significantly. Therefore, it is crucial to determine which antivirus program is best suited to a particular user's needs. The goal of this thesis is to investigate the effectiveness of four leading antivirus software programs, including Kaspersky, Bitdefender, ESET, and McAfee. The study will assess the performance of these programs through a performance test and an evaluation using the Saaty’s method, which involves comparing the relative importance of evaluation criteria.

The performance test will involve evaluating the programs' ability to detect and remove malware, their scanning speed, and their impact on system performance. The evaluation using the Saaty’s method will consider factors such as the programs' ease of use, cost-effectiveness, and customer support. By comparing and contrasting the performance of these programs, this research aims to provide valuable insights for individuals and organizations seeking to improve their cybersecurity posture.

The study will begin by providing an overview of the cybersecurity landscape, including the various types of cyber threats, their impact on individuals and organizations, and the role of antivirus software in combating them. Next, the study will review the literature on antivirus software, including the different types of programs available, their features, and their effectiveness. The study will then describe the methodology used to evaluate the antivirus programs, including the performance test and the Saaty’s method. Finally, the study will present the findings and conclusions, highlighting the strengths and weaknesses of each program and providing recommendations for individuals and organizations seeking to enhance their cybersecurity posture.

In summary, this thesis aims to provide valuable insights into the effectiveness of four leading antivirus software programs, including Kaspersky, Bitdefender, ESET, and McAfee, through a performance test and an evaluation using the Saaty’s method. By evaluating the performance of these programs, this research seeks to help individuals and organizations make informed decisions about which antivirus program is best suited to their needs and enhance their cybersecurity posture.

2 Objectives and Methodology

2.1 Objectives

This thesis investigates the field of the antivirus branch in cyber security. The thesis aims to analyze the antivirus programs, and tools in cyber security. The partial objectives of the thesis are:

- to characterize the fundamentals of cybersecurity,
- to identify possibilities of researched and found antivirus programs,
- to compare the found antivirus programs, review of surveys and interviews,
- to evaluate the surveys and interviews found.

2.2 Methodology

The methodology of this thesis will be divided into two parts. The first part will introduce cybersecurity, followed by a discussion on the role of antivirus software in cybersecurity. One of the main objectives of this thesis, which is to explain what antivirus software is and what it means, will also be discussed in this section. The second part of the thesis will compare the performance tests and independent surveys of the most commonly used antivirus programs worldwide, using the Saaty's Method to score the results. Additionally, interviews with the managers of the identified antivirus programs will be included.

3 Literature Review

3.1 Introduction to Cybersecurity

Cybersecurity encompasses the utilization of technologies and processes to safeguard electronic and computerized data from unauthorized access or theft. This umbrella term includes various elements such as software, hardware, communication infrastructures, and human actions. The concept of cybersecurity can be modified to fit any security issue that may arise, given that its boundaries are not yet distinctly defined. The threat landscape of cybersecurity is in constant evolution, and attackers are increasing in sophistication with their methods. Malware refers to software that is intentionally created to damage or exploit a system or network, including viruses, worms, Trojan horses, and other software utilized for data theft, system control, or operational disruption. Phishing is a social engineering attack that deceives a user into disclosing sensitive information by impersonating a reliable entity. Common forms of cyber threats comprise malware, phishing, denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, man-in-the-middle (MITM) attacks, and advanced persistent threats (APTs). The primary objective of DoS and DDoS attacks is to flood a system or network with traffic or requests, making it unavailable to legitimate users. MITM attacks involve intercepting and modifying communication between two parties, allowing for eavesdropping or data theft. APTs are complex attacks intended to infiltrate a system or network and remain undetected for extended periods, allowing attackers to obtain access to sensitive information or systems. [1]

Data can contain confidential information belonging to commercial entities or individual users, among other things. Cybersecurity involves adopting measures that protect computer networks from software and data attacks, as well as unauthorized use and damage. As we continue to move our daily activities online, cybersecurity has become a rising concern for both businesses and individuals. To combat the various forms of cyber threats, there are multiple types of cybersecurity measures that can be put in place. Network security concentrates on safeguarding computer networks from misuse, attacks, and unauthorized access.

In order to safeguard against threats, it is crucial to prevent unauthorized access to systems and data. There are numerous measures that businesses and individuals can take to enhance their cybersecurity. Some of the risks involved can be categorized as cyber threats, which come in various forms such as malware, phishing, hacking, and ransomware. Cyber threats are aimed at exploiting vulnerabilities in computer systems to steal sensitive information or cause damage to the system. Cybersecurity measures seek to prevent such threats from occurring, identify them when they do, and respond efficiently to minimize the impact. One of the biggest challenges in cybersecurity is keeping up with the rapidly evolving threat landscape. Cybercriminals are continually developing new and sophisticated methods to breach security systems, making it crucial for cybersecurity experts to be proactive in their efforts to protect against cyber threats. This necessitates ongoing training and education, as well as collaboration across organizations and industries to share information about emerging threats and best practices for preventing and responding to them. [2]

Additionally, it is important to be aware of the latest cyber threats and know how to identify their email or other attempts to gain access to sensitive information. By taking these few measures, we can all help make the internet we use safer for everyone. Ensuring the prevention of data breaches, identity theft and hacking is important for individuals, businesses and governments to protect their confidential information and prevent attacks that can disrupt operations. There are disposables to improve cybersecurity such as using strong passwords, using antivirus programs, encrypting data and installing firewalls, but even these may not be enough. Organizations should implement strong authentication measures such as two-factor authentication and ensure that employees use unique passwords for each account. They must also encrypt all their sensitive data using industry-standard encryption algorithms and at rest in transit. [3]

As has been demonstrated, cybersecurity is an increasingly important concern in our digital world. With the increasing dependence on digital technologies, the risks associated with cyber threats and data breaches continue to grow. To protect against these risks, organizations and individuals must implement effective cybersecurity measures that include a combination of technical and non-technical controls, ongoing education and training, and collaboration across organizations and industries. By taking proactive measures to protect against cyber threats, we can ensure a safer and more secure digital future.

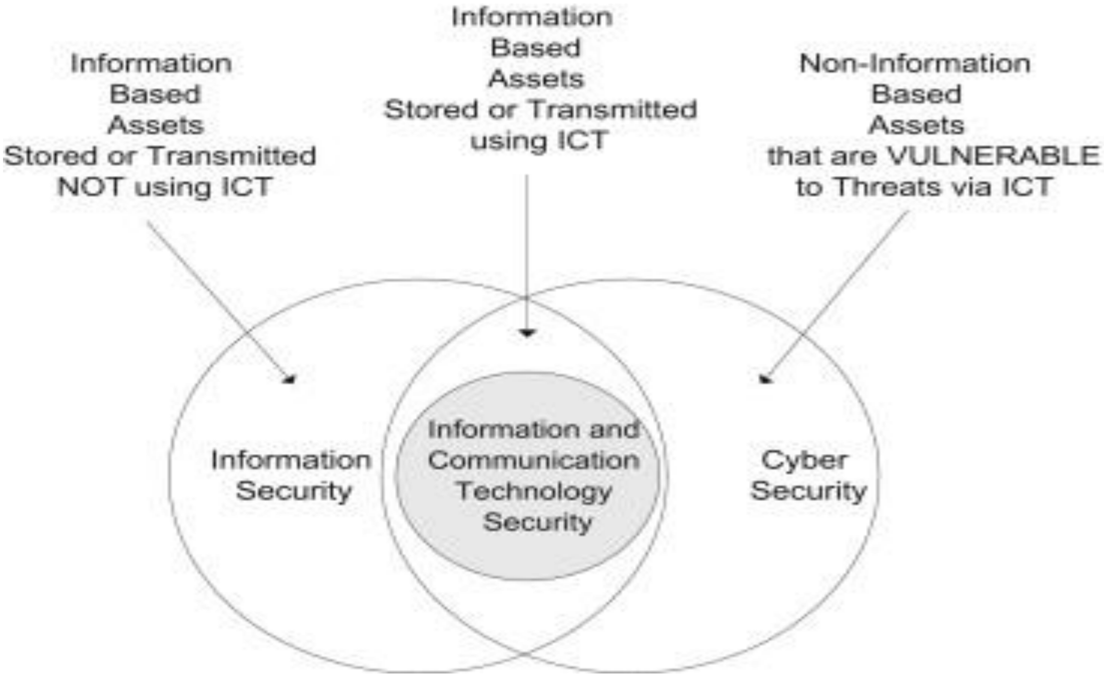

Information Based Assets Stored or Transmitted NOT using ICT
Information Based Assets Stored or Transmitted using ICT
Non-Information Based Assets that are VULNERABLE to Threats via ICT
Information Security
Information and Communication Technology Security
Cyber Security

Figure 1: Cyber Securiy and Informantion Security Connection Table [4].

3.1.1 Types of CyberSecurity

3.1.1.1 Application Security

Application security is critical to protecting your organization from cyberattacks. It can help protect your data and prevent unauthorized access to your systems by implementing strong security measures. A wide variety of application security solutions are available, and it's important to choose the right one for your needs. An effective application security strategy and firewall systems should include multiple layers of defence in encryption. Safe practices must be designed to minimize such cybersecurity incidents. [5]

3.1.1.2 Data security

Data security is the practice of protecting electronic information against unauthorized access. It includes both physical and logical security measures. Physical security measures protect the hardware that stores the data, while logical security measures protect the data itself. Data Security is essential for organizations of all sizes to protect confidential information and maintain customer trust. [6]

3.1.1.3 Network Security

Network security is a process that helps protect your computer networks and data from unauthorized access or theft. It includes measures to prevent, detect and respond to attacks. Network security has many benefits, including the ability to prevent data loss or theft, protect privacy, and ensure business continuity. In today's connected world, it is more important than ever to have strong network security measures in place. [7]

3.1.1.4 Critical infrastructure security

Critical infrastructure security is a top priority for any government. The consequences of an attack on critical infrastructure can be huge, and the potential for damage increases as our society becomes more reliant on technology. There are many steps governments can take to improve critical infrastructure security. They must improve intelligence collection and analysis, plan for response and recovery, and plan for potential threats. [8]

3.1.1.5 Cloud Security

Cloud security is a growing concern for businesses and individuals alike. As more data is stored in the cloud, the potential for data breaches and other security issues increases. While cloud providers have taken steps to improve security, there are still many vulnerabilities that need to be addressed. Businesses need to carefully consider their options when choosing a cloud provider. They need to make sure that the provider has robust security measures to protect their data. Individuals should also be aware of the risks of storing their data in the cloud. A well-known provider should choose a strong password, and one of the most important is two-factor authentication. [9]

3.1.2 Exploring the Scope of Cyber Security Implementation

The term "cybersecurity" pertains to the protection of electronic data and systems against unauthorized access or theft. It can cover personal data stored on a computer or sensitive company information transmitted over the internet. [10] There are many different ways to protect electronic data, and the level of protection required varies depending on the type of information involved.

As cyberattacks become more sophisticated, businesses need to invest in strong cybersecurity measures to safeguard their assets and their customer's data. Protection can involve password protection, antivirus programs, encryption, firewalls, and intrusion detection systems, among other things.

Several factors should be taken into consideration when developing a cybersecurity strategy, such as the types of threats faced, business goals, and budget constraints. While cybersecurity is mainly focused on electronic data protection, it also has critical implications for physical security. For instance, critical infrastructures such as power plants or water treatment plants can be vulnerable to hacking, which can have severe consequences for public health and safety. As technology becomes more ubiquitous in our lives, it is crucial to ensure that we have adequate protection against potential cyber threats. [11]

3.1.3 The Significance of Cyber Security in Today's World

In today's digitally-driven world, cybersecurity is a critical component of both personal and professional life. With the increased reliance on technology and the internet, protecting ourselves from potential cyber threats is essential. Cybersecurity measures can help prevent identity theft, financial fraud, and other types of cyberattacks. [12]

Moreover, businesses must also be vigilant about cybersecurity. Confidential information, such as financial records, trade secrets, and customer data, are stored on their computers and networks, and a breach can have serious repercussions. A cyberattack on a company can lead to sensitive data being leaked or stolen, resulting in damage to the company's reputation and financial losses. Therefore, businesses should take measures to enhance their cybersecurity efforts.

To improve cybersecurity, individuals and companies can implement various measures. For instance, strong passwords, two-factor authentication, and encryption can help protect personal and corporate data. Additionally, regular software updates and security patches can fix known vulnerabilities that hackers could exploit. Furthermore, businesses should conduct regular cybersecurity assessments, penetration testing, and employee training to ensure that their systems and employees are up-to-date with the latest security protocols. [13]

In conclusion, cybersecurity is crucial in today's world as it helps protect both individuals and businesses from potential cyber threats. By implementing appropriate cybersecurity measures, we can ensure that the internet remains a safe place for everyone to work, play, and communicate. [14]

3.1.4 Cyber Security and Data Protection: Advantages for Individuals and Society

As digital operations and the internet continue to evolve and change, cybersecurity practices must also adapt to keep pace with emerging threats. The greatest benefit of top-tier cybersecurity solutions is that they provide a comprehensive shield for individuals and organizations, safeguarding against cyber threats. Such solutions identify new vulnerabilities, educate the public about the importance of cybersecurity, and strengthen open-source tools. [15] By taking steps to secure their networks and user data, businesses can minimize the risk of costly downtime and data loss while preventing potential reputational damage from a security breach or attack. Ultimately, their efforts help to make the internet a safer place for everyone.

The significance of cybersecurity lies in its ability to protect individuals and organizations from a wide range of cyber threats. A robust cybersecurity strategy should include firewalls, antivirus programs, intrusion detection systems, encryption technologies, and strong authentication procedures to create a multi-layered defense against sophisticated attackers. As cybercrime continues to rise, it is more important than ever to prioritize cybersecurity measures to avoid potentially devastating consequences, such as the loss of sensitive information, financial loss, or damage to reputation. [16]

In essence, effective cybersecurity practices are necessary to safeguard against the evolving threat landscape and protect individuals and organizations from cyber threats. By implementing robust cybersecurity measures, businesses can reduce risk, increase protection, and ensure the safety and security of their networks, user data, and the broader digital environment.

An effective cyber security strategy, firewalls, antivirus programs, intrusion detection systems (IDS), encryption technologies, and strong authentication procedures, such as multiple layers of Defense must contain. By implementing these measures, businesses can create a solid defence against even the most sophisticated attackers. The rate of cybercrime is increasing; therefore, it is very easy to lose sensitive information, money or reputation without cyber security. Cyber security is as important as the need for technology.

Ensuring cyber security; protects the person, protects the institution, protects productivity and efficiency, prevents websites from crashing, and protects against spyware. [17] The main protection benefits are will be mentioned below;

- Protection against malware, ransomware, phishing and social engineering,
- Protection for data and networks,
- Prevention of unauthorized users,
- Increases the recovery time after the violation,
- Better system performance,
- More product confidence for developers and customers alike.

3.1.5 Cybersecurity and Data Privacy: Protecting Sensitive Information from Threats

There are many dangers associated with malicious cybersecurity. Hackers can access personal information such as social security numbers and credit card information. They can also infect computers with viruses and malware. This can lead to identity theft, financial loss and loss of privacy. In some cases, hackers have even managed to take control of critical infrastructures such as power plants and hospitals.

Malicious cybersecurity can have a ripple effect across the entire organization. For example, if an employee's computer is hacked, the hacker may have access to the company's network. This could lead to a data breach that exposes sensitive customer or customer information. A cyberattack can also disrupt operations by crashing vital systems or holding them for ransom. The loss of reputation of a company from such an event can be a big problem for a large company. [18] The main damages are will be mentioned below;

- Hackers gaining access to people's personal information.
- Hackers find a vulnerability and break into any company
- Theft of important data
- Sending malware
- Malicious financial gain
- Sabotage, espionage and system and network damage

3.2 Cyber Security Threats and Trends: A Comprehensive Overview

In today's rapidly evolving technological landscape, cybersecurity threats are becoming increasingly pervasive, underscoring the critical importance of awareness and taking proactive measures to safeguard oneself. Among these threats, malware poses a formidable danger to computer systems, utilizing diverse vectors like email attachments, websites, and social media links to gain unauthorized access. Once it infiltrates a device, malware can cause a range of severe consequences, from pilfering confidential information to irreversibly deleting essential files or even assuming total control of the system.

Another prevalent form of cybersecurity threat is phishing, which involves cybercriminals masquerading as trusted websites or organizations to deceive unsuspecting victims into revealing sensitive information. For example, attackers may create emails that closely resemble official messages from a victim's bank, soliciting them to update their account information or directing them to counterfeit websites designed to steal login credentials.

Consequently, it is imperative to remain well-informed and take appropriate measures, such as utilizing reliable antivirus software, scrutinizing suspicious emails, and avoiding clicking on dubious links, to mitigate the risks posed by these insidious threats. [19] [20] [21]

3.2.1 Cyber Security Threats Types

3.2.1.1 Denial-of-service attack (DDoS)

A DDoS attack is a cyberattack that floods a computer or network with traffic from multiple sources, making it unusable for legitimate users. Attackers can achieve this by sending too much data for the system to process or filling the destination with data requests. In both cases in the Figure 2, the goal is to make the system unusable for legitimate users. [22]

3.2.1.2 Malware

Malware is a term used to describe software programs and code that are designed to harm or disrupt digital devices, networks, and computers. This can include viruses, which are self-replicating programs that can spread from one device to another, spyware, which collects data without the user's consent, Trojans, which masquerade as legitimate software but contain harmful code, and ransomware, which locks users out of their systems or encrypts their files in exchange for payment. It is important to use antivirus software, practice good online hygiene, and establish strong cybersecurity policies to protect against malware attacks. One of them is Spyware. Spyware collects information without a user's knowledge or consent and uses it maliciously. As you can see the Figure 2 that antivirus software was also created to protect them. [23]

3.2.1.3 Phishing attack

Phishing attacks, as shown in Figure 2, are fraudulent attempts to obtain sensitive information by tricking users into believing that they are communicating with a trustworthy source. Phishing attacks can be very difficult to detect. These attacks are difficult to detect but some indicators include poor grammar or spelling errors, and requests for personal information. In case you receive an email or message that appears suspicious, do not respond to it, and report it immediately to your IT department or security team. [24] [25]

3.2.1.4 Cryptojacking

Cryptocurrency mining involves verifying transaction records and adding them to the blockchain, with miners receiving cryptocurrency as a reward. However, cryptojacking is the unauthorized use of someone else's computer to mine cryptocurrencies without their knowledge or consent. It's a common form of theft, as finding an IP address in cryptocurrencies is challenging. To prevent cryptojacking, it's crucial to install security software and keep it up to date. Additionally, users should avoid clicking suspicious links or downloading unknown software, as these may contain malware that can lead to cryptojacking. [26]

3.2.1.5 Insider Threats

An insider threat refers to a cybersecurity risk from within a company in Figure 2. Insider threats pose a significant cybersecurity risk that originates from within a company, often due to employee actions. The most significant danger of insider threats is data leakage, which can happen when individuals intentionally or unintentionally disclose sensitive information. Insider threats can also take various forms, including intellectual property theft, system sabotage, and unauthorized access to confidential information. To reduce the risk of insider threats, companies should implement security measures such as access controls, monitoring systems, and employee education and training programs. Maintaining vigilance in monitoring and addressing insider threats is crucial for protecting data, reputation, and bottom line. Fostering a culture of security awareness and ethical behavior among employees is essential to mitigate insider threats. [27]

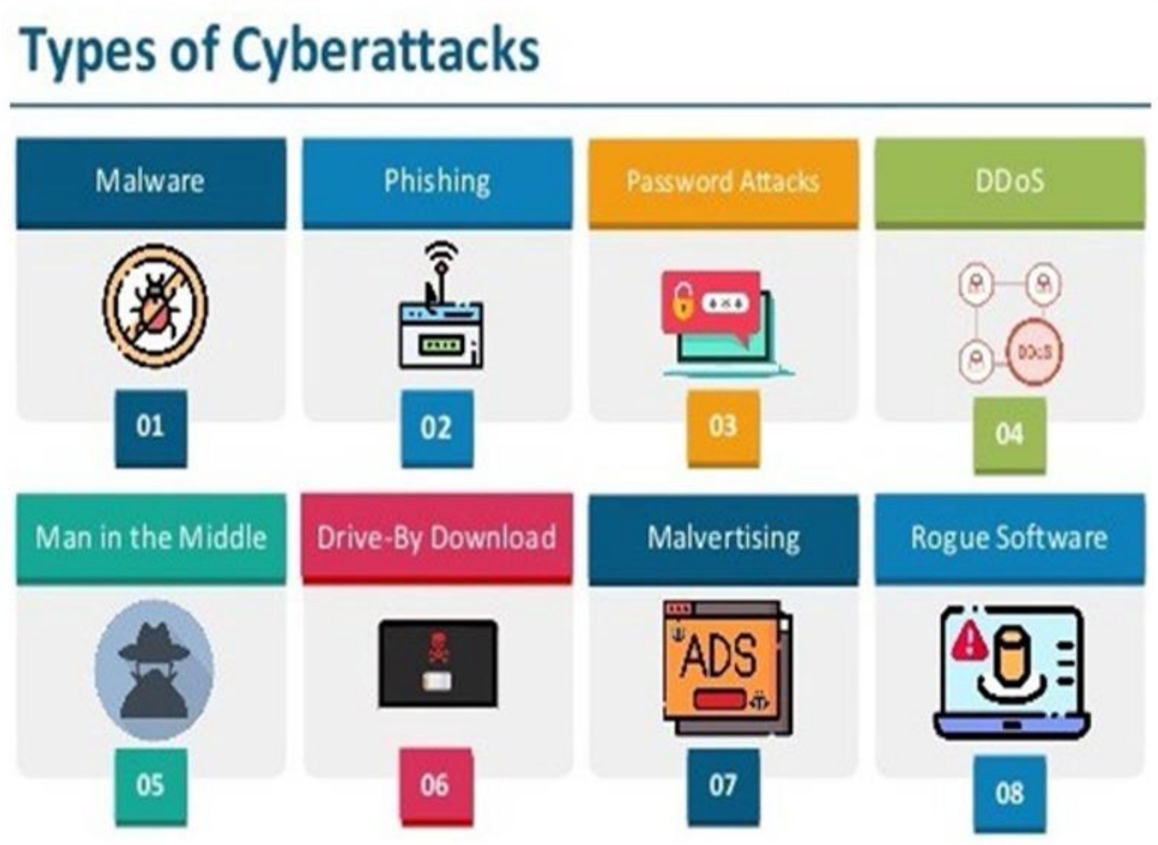


Figure 2: Types of Cyber Attacks table [28].

3.2.2 Information Security: Understanding the Importance of Protecting Confidentiality, Integrity, and Availability

There are very similar features between cyber security and information security. A lot of information entering the field of cyber security includes information security with the development of technology today. Information security, also known as cybersecurity or IT security, is the protection of electronic information from unauthorized access or theft. In recent years, with the increase in computer and internet usage, information security has become more and more important. There are many different types of information security, including data encryption, firewalls, and password protection. [29]

Information security is the practice of protecting electronic information by reducing information risks and vulnerabilities. Information risks may include unauthorized access, data use, disclosure, interference or destruction of data. Data may include, but is not limited to, confidential information of commercial or individual users. Vulnerabilities can be caused by weak passwords, system design flaws, and social engineering techniques. To protect data, organizations and individuals can implement security measures such as access control systems, encryption technologies, and physical security measures. [30] [31]

3.2.3 Information Security and Cybersecurity in Practice: Examining the Differences in Implementation

Focusing on information in the name of information security, the field of security covers not only digital information but also analogue information. That is, it covers any environment where information is available. It doesn't have to be digital, but when we say cyber security, cyber security covers all digital channels. It covers the infrastructure systems on which digital media work and talks about their security. Today, there is a similarity between the digitalization of information and information security and cyber security. This makes the distinction between similarities a little more difficult. What we are talking about fundamentally in cyber security is not information. Systems that transport information, systems that produce information, and systems such as the IoT. Therefore, there is a very different scope of cyber security in the digital environment. The most important difference is that security is not limited to information only. It varies according to the needs of the companies.

3.2.4 Analytic Hierarchy Process (AHP) and Saaty’s Method: A Comprehensive Guide

The Analytic Hierarchy Process (AHP) is a decision-making framework developed by Dr. Thomas L. Saaty in the 1970s. It is a mathematical approach to decision-making that allows decision-makers to prioritize and compare different options based on a set of criteria. "The essence of decision making is not the thinking process itself, but the actions that flow from the thinking." He said [32]. The AHP is widely used in business, engineering, and other fields where complex decisions need to be made. [33]

The Saaty’s Method, named after Dr. Saaty’s, is the underlying methodology used in the AHP. It is based on the principle that all decision-making involves trade-offs between multiple criteria. The Saaty’s Method provides a systematic way to evaluate these trade-offs and make informed decisions. The AHP process involves four steps:

Step 1: Define the decision problem and the criteria to be considered. This step involves identifying the decision problem and breaking it down into a set of criteria that will be used to evaluate the options.

Step 2: Develop a hierarchy of the decision problem. This step involves organizing the criteria into a hierarchy with the most important criteria at the top and the least important criteria at the bottom. This helps decision-makers to visualize the decision problem and the relationships between the criteria.

Step 3: Determine the relative importance of the criteria. This step involves pairwise comparisons of the criteria. Decision-makers compare each criterion to every other criterion and assign a relative weight or importance to each criterion.

Step 4: Evaluate the options. This step involves evaluating each option against each criterion and assigning a score. The scores are then weighted according to the importance of the criteria to determine the overall ranking of the options.

The Saaty’s Method is used in Step 3 of the AHP process to determine the relative importance of the criteria. The Saaty’s Method involves creating a matrix of pairwise comparisons for each criterion. Decision-makers are asked to compare each criterion to every other criterion and assign a score based on their relative importance. The scores are then normalized to create a matrix of weights that can be used to determine the overall importance of each criterion.

The AHP and Saaty's Method have several advantages over other decision-making methods. They provide a structured and systematic approach to decision-making that ensures all relevant criteria are considered. They also allow decision-makers to incorporate both quantitative and qualitative factors into the decision-making process.

Considering all of the facts, the Analytic Hierarchy Process (AHP) and Saaty's Method are powerful decision-making tools that can help decision-makers prioritize and compare different options based on a set of criteria. By using a systematic and structured approach, decision-makers can make informed decisions that take into account all relevant criteria. [33]

3.3 Introduction to Antivirus Systems

Antivirus software is a computer program that helps protect your computer from viruses and other malware. Antivirus systems are designed to protect the essential information people have on their computers. This software is the most important part of your computer's security system and you must keep it up to date. Antivirus software works by identifying and eliminating these threats before they cause any damage to your computer. Antivirus software can be used to prevent or remove malware, including spyware, adware, worms, and viruses. If any person accidentally installs the antivirus software on his computer, even if he accidentally uploads an infected site or an infected file, the antivirus program prevents the harmful virus from infecting the computer and essential information on people's computers will not be stolen. Antivirus programs not only protect information on your computer but also offer other features such as email filtering and anti-phishing.

Many different antivirus programs are available for both home and business users. There are also many different antivirus programs, and it's important to choose one that will work well with the operating system you're using. It is important to keep your antivirus program up to date to effectively protect your computer from the latest threats. Although some users complain about these updates, they are quite important. The reason is that a new generation of malware is constantly being created. Companies that detect these update the program as a solution. Some antivirus programs are free, while others must be purchased.

There are also some that come preinstalled on new computers. Some of the most popular antiviruses are ESET AntiVirus, McAfee VirusScan, Kaspersky Lab Anti-Virus, Bitdefender Antivirus Plus. When choosing an antivirus program for your computer, it's important to choose one that offers real-time protection against new threats and regular updates to keep virus definitions up to date. Although most people look at the prices first, it should be known that this is not such an easy thing. When choosing an antivirus program, the first thing to consider is not the price, but the area that the antivirus program will protect.

While many antivirus programs look cheap, they actually have that low of protection. Because of this, antivirus companies have gained a lot of customers. But there are many complaints.

But, unfortunately, antivirus companies cannot help in this regard as it is an antivirus program that people choose voluntarily. While the package that people choose cannot provide 100% protection against all threats because it is a single piece of security software, using a quality antivirus program is an important part of protecting your computer from malware infections. It also needs to run regular scans of your computer using antivirus software to detect any malware that might have gotten past its defences. Although many computer users thought that the antivirus programs they installed on their computers would protect them completely, it is not so easily possible. Antivirus programs can only protect your computer as long as they are kept up-to-date. In addition, it may not be possible for antiviruses to catch a virus that has not yet been recognized and spread by antiviruses. This also varies depending on the antivirus program purchased. Therefore, it is extremely important for everyone who uses a computer to be aware of this issue. Companies that sell antivirus programs do not provide much information on these issues. They argued that they did this with the knowledge of the users. [34] This is why many users have purchased without reading the detailed usage agreement. As I mentioned before, many users have suffered. In order not to encounter a situation like these examples, the protected areas of antiviruses should be examined in detail and compared with other antivirus programs and choose the most appropriate antivirus program. [35]

3.3.1 The Significance of Antivirus Programs in Protecting Personal and Corporate Information Security

The security of computers is provided by antivirus software programs. If this security measure is not provided, your computer becomes vulnerable to virus threats, especially through your internet connections. In addition, it is very likely that we will be exposed to viruses from devices that are connected to the computer with an external cable, such as USBs, external hard drives and SD cards. Devices without an antivirus program will be vulnerable to malicious viruses from outside. Viruses are like harmful substances with the same name that threaten your body. This small-sized and malicious software can enter your computer and prevent your device from working properly to document and capture your essential data and may cause negative situations by sending harmful data, files or e-mails to your computer. While it sometimes causes major or minor damage to your computer that can be repaired, it can sometimes cause irreversible major problems.

Using antivirus programs helps you secure your computer and data. In this way, you can have a computer free from harmful effects and ensure the security of your data. By using your device for many years, you can achieve internet usage free from cyber attacks and viruses.

3.3.2 The Mechanics of Antivirus Software: An Overview of its Core Functions and Features

Antivirus programs use various methods for their primary purpose, such as finding viruses, and quarantining/deleting them. These methods determine the working system of antivirus programs. Computers may be under threat of damage by bad hackers. These damages usually occur as a result of malicious software entering your computer over the internet or from external memory inserted into the computer. It makes antivirus programs to protect the computer from all viruses, prevent them from entering the system, and find, block and clean existing viruses if any. Therefore, many people have started to use antivirus programs against threats.

The intensity of cyber attacks is increasing day by day. Installing these programs that help protect your computer from viruses will make your life much easier. In this way, you will be sure that your data does not fall into the hands of malicious people, and you will ensure that your computer remains healthier. In this way, you will protect both yourself and your loved ones from harmful cyber effects, and most importantly, you will ensure cyber security. [36]

3.3.3 Antivirus Policies and Procedures

Antivirus policies and procedures are commonplace, especially for businesses to protect their computers. These policies and procedures are designed to avoid exposure to any virus or malware. Depending on these policies and procedures implemented with antivirus programs, mechanisms have been developed to help effectively detect damage on computers. Compliance with such policies is vital in keeping data safe and protected from cyber threats.

Antivirus policies and procedures; While helping to provide an effective defence against viruses, it also provides support to administrators. It also helps mitigate the damage caused by these threats if they manage to infiltrate a system or network. To ensure that antivirus protection is effective in protecting against potential threats, organizations must have clear policies and procedures regarding their implementation and use.

3.4 ESET Antivirus Program

ESET antivirus programs are one of the most reliable and effective security software today. With its cutting-edge technology, ESET provides users with comprehensive protection against a variety of threats, including malware, ransomware, and viruses. Its user-friendly interfaces make it easy for anyone to get up and running quickly while continuing to offer advanced features to those who need them.

The main advantage of using an ESET program is its high detection rate compared to other antivirus solutions on the market. This means that your system will be protected against malicious threats before they have a chance to harm or damage your data or device in any way. Additionally, these programs offer additional layers of protection, such as anti-phishing features that can help you stay safe online even if you accidentally click on a malicious link or download something potentially dangerous from the internet without knowing firsthand. [37]

Initially, since the system of equipping with antivirus programs will help to reduce the risk of infection in the device, it should be ensured that the necessary hardware materials are provided by taking safety precautions. Developing an antivirus programming strategy will help you evade any cyber threat. In the first step; They should look at which of the available equipment is the most effective. You should try to get daily updates to perform detailed scans so that the latest virus versions can be caught. In the next step, incompatibilities arise as the prices of antivirus programs, which is one of the points to be considered when it comes to choosing antivirus software, come to a disturbing level. Then, before starting the integration, they should complete a detailed examination of the relevant hardware, get technical support from the company that carries it, and make suggestions.

Finally, another great advantage of using an ESET program is the customer support team that offers 24/7 assistance in case of any problems during or after installation. This gives users the comfort of knowing someone is available should they run into any issues to protect themselves from cybercrime. Choosing an ESET product for your computer's security needs will ensure maximum security no matter what threat comes.

Ultimately; Before commissioning and testing the antivirus program, they should open a virtual machine and do all the tests. They should try the policies and procedures of all Antivirus programs one by one, and the response editor, namely (ACD) should be set and checked. [38]

3.5 Kaspersky Antivirus Program

Kaspersky antivirus programs are one of the most popular and reliable security solutions available on the market today. Kaspersky offers a wide selection of products to protect users from various types of threats, including viruses, malware, spyware and ransomware. The company has been providing highly reliable protection for over many years and is an antivirus program integrated with advanced technologies to help users stay safe online.

Kaspersky has several award-winning antivirus programs. It provides multiple layers of defence against malware by scanning any of them in real-time as they are downloaded or opened on your computer. It also monitors incoming malicious virus traffic and provides network attack blocker technology to detect suspicious activity before it does any damage to your system or data files. Additionally, Kaspersky's anti-phishing feature is also a Safe Money Technology that encrypts transactions to protect all financial attacks through banking, while surfing any website securely with browser extension tools such as usernames by (hackers) hackers and helps protect you from fake websites that could be used to steal personal data such as passwords. These websites or e-commerce stores provide a safeguard so that no one else can access them, even if they somehow manage to get hold of your personal data.

Finally, Kaspersky customer support team is always there for you 24/7 when you need help, whether it's troubleshooting a problem with one product or getting advice on another product, and ensures that every user's security solution is the best possible, no matter what device they are using. Enable them to gain experience. (Windows PC/Mac/Android). All in all, choosing a reliable antivirus program like Kasperksy provides maximum protection against cyber threats. At the same time, letting users know that their data is always safe, and you can put their information very comfortably. [39]

3.6 McAfee Antivirus Program

McAfee antivirus programs are one of the most reliable and comprehensive security solutions available on the market today. Offering complete protection against viruses, malware, ransomware, spyware and other threats, McAfee has provided users with peace of mind for over 30 years. McAfee offers comprehensive protection for home users and businesses of all sizes. Its products range from basic anti-virus suites to advanced endpoint security solutions that protect against sophisticated malware attacks. [40]

McAfee's products are designed with ease of use in mind. It offers a range of features that can be tailored to suit individual needs or business needs, such as real-time scanning, automatic updates, web browsing control tools, and more. They can be installed quickly and easily on any device with minimal user effort. In addition, its real-time scans ensure that your system is always protected, no matter what threat you encounter online. In addition, advanced features such as firewall protection help protect your data even when you are not actively using it. Overall, McAfee antivirus programs offer reliable protection with powerful features at competitive prices, making them an excellent choice for both home users looking for essential virus protection and businesses looking for advanced security measures against cyber threats like ransomware attacks.

Finally, McAfee offers various subscription plans tailored to suit different budgets. Combining all these features in one package, consumers looking for reliable antivirus software solutions choose McAfee's number one antivirus for this reason. [41]

3.7 Bitdefender Antivirus Program

Bitdefender Antivirus Program is one of the leading security solutions available on the market today. The company has been providing comprehensive security solutions since 2001, and its products have consistently received top marks from independent testing labs around the world. It offers a suite to protect users from malware and threats, including viruses, spyware, and more. Bitdefender's antivirus programs provide comprehensive protection against all types of malware while offering advanced features such as parental control options and secure file-sharing capabilities not often seen in other antivirus programs.

We can name a few main features that make Bitdefender different, the latest version of Bitdefender's flagship product includes an artificial intelligence engine that can learn from experience to identify potential threats faster than ever. This method is unprecedented in traditional antivirus software. The unique "Autopilot" mode allows users to set up automatic scans so that users do not have to manually run them every time their computer is turned on or restarted. This means that even when you are away from your computer, it will be protected by a potent virus detection engine that uses artificial intelligence technology for maximum accuracy before potential threats do any damage or disrupt your system. This event allows it to quickly scan the files on your computer or device for any suspicious activity without degrading performance or affecting battery life too much. Additionally, cloud integration means you'll get up-to-date virus definitions whenever you need them, so your system is always safe no matter where you connect. [42]

In summation, if you want maximum protection against malware, then BitDefenders Antivirus Program will be more beneficial than other antivirus packages. It provides comprehensive coverage with ease of use, perfect for both novice and novice users, thanks to both its Autopilot mode and intuitive user interface design.

4 Practical Part

4.1 A Study on the Effectiveness of Antivirus Software in Detecting Malware: A Comparative Approach

Antivirus programs are essential in protecting computers and networks from various types of malware such as viruses, worms, Trojans, and other malicious software. With the abundance of antivirus programs available in the market, it is important to compare and contrast their features to determine which one best suits your needs.

In recent years, numerous research firms have conducted tests on antivirus programs, and their results have been made public. However, it is also essential to consider whether the antivirus program is meant for personal or business use. In my own research, the most popular antivirus programs used globally in the last five years are Kaspersky, Bitdefender, McAfee, and ESET, respectively.

When comparing antivirus programs, it is crucial to evaluate their proactive and reactive capabilities. Proactive antivirus programs are designed to prevent malware attacks by identifying and blocking them before they can harm the computer or network. On the other hand, reactive antivirus programs are designed to detect and eliminate malware after it has infected the system.

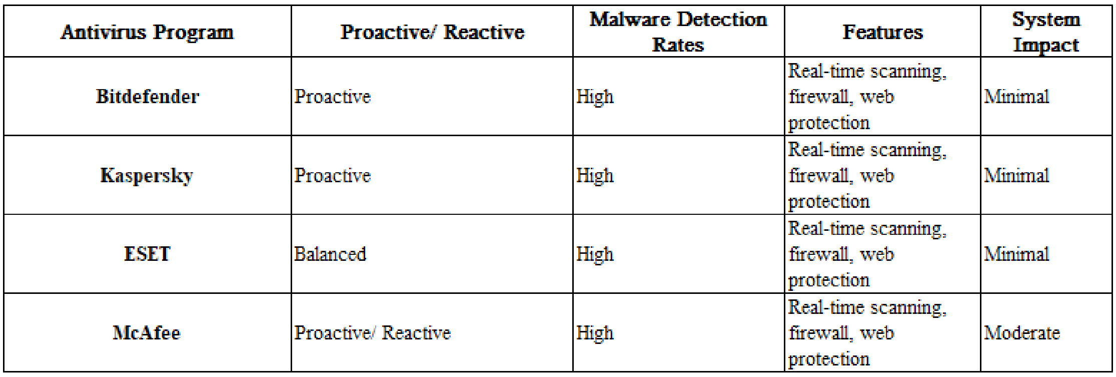
Based on my research, Bitdefender is the best proactive antivirus program in terms of features and overall performance. The program consistently receives high ratings in independent tests for its malware detection and blocking capabilities. Bitdefender is also easy to use and has a minimal impact on the computer's performance.

Kaspersky is another top-performing antivirus program that offers comprehensive protection against malware. It has robust features such as real-time scanning, a firewall, and web protection. Kaspersky's malware detection rates are also high, making it a reliable option for both personal and business use.

ESET is a lightweight antivirus program that offers a balance of proactive and reactive features. It is easy to use and has a minimal impact on system performance. ESET's malware detection rates are also high, making it a popular choice for personal use.

McAfee is a reputable antivirus program that provides users with comprehensive security features such as real-time scanning, a firewall, and web protection. However, its performance impact on the system is relatively higher than the other antivirus programs mentioned in this article.

To better compare the four antivirus programs, we have created a table below:



Antivirus Program	Proactive/ Reactive	Malware Detection Rates	Features	System Impact
Bitdefender	Proactive	High	Real-time scanning, firewall, web protection	Minimal
Kaspersky	Proactive	High	Real-time scanning, firewall, web protection	Minimal
ESET	Balanced	High	Real-time scanning, firewall, web protection	Minimal
McAfee	Proactive/ Reactive	High	Real-time scanning, firewall, web protection	Moderate

Table 1:Proactive or Reactive table of Antiviruses

As we can see from the table above, all four antivirus programs offer high malware detection rates and comprehensive features such as real-time scanning, a firewall, and web protection. However, Bitdefender and Kaspersky are purely proactive antivirus programs, while ESET offers a balance of proactive and reactive features. McAfee, on the other hand, offers both proactive and reactive features but has a more significant impact on system performance.

In terms of features, all four antivirus programs offer similar capabilities, such as real-time scanning, a firewall, and web protection. However, Bitdefender and Kaspersky stand out for their consistently high malware detection rates, making them reliable options for both personal and business use.

ESET offers a lightweight and easy-to-use interface, making it popular among personal users. McAfee offers a comprehensive suite of security features but may have a more significant impact on system performance.

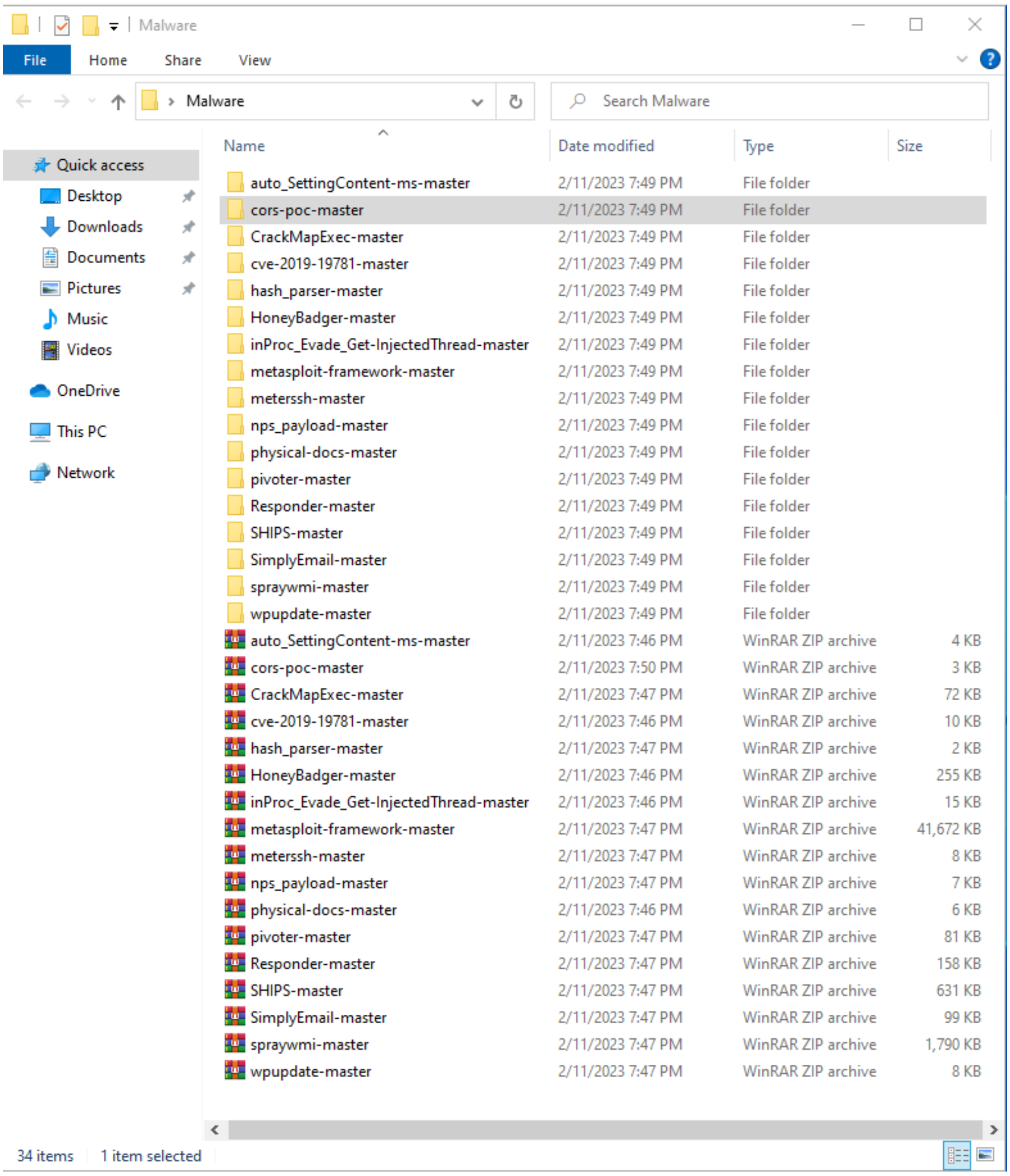
When it comes to system impact, Bitdefender, Kaspersky, and ESET have minimal performance impact on the system. However, McAfee's impact on system performance is relatively higher than the other antivirus programs mentioned in this article. Therefore, users who have lower system specifications may experience lag and slower performance when using McAfee.

To finalize, choosing the best antivirus program for personal or business use can be a challenging task. It is crucial to compare the features, proactive and reactive capabilities, malware detection rates, and system impact of each antivirus program to determine which one best suits your needs. Based on my research, Bitdefender and Kaspersky are the best antivirus programs for both personal and business use due to their consistently high malware detection rates and comprehensive features. ESET offers a lightweight and easy-to-use interface, making it a popular choice for personal use. However, McAfee's performance impact on the system is relatively higher than the other antivirus programs mentioned in this article, making it less suitable for users with lower system specifications.

Bitdefender, Kaspersky, ESET, and McAfee are all reliable antivirus programs that offer comprehensive protection against malware. Each program has its strengths and weaknesses, and users should carefully evaluate their needs and preferences before choosing an antivirus program. Regular updates, safe browsing habits, and additional security measures can help maximize the effectiveness of your chosen antivirus program in protecting your computer and network from malware attacks.

4.2 The Impact of Harmful Viruses Found on the Internet: A Case Study

After setting up a virtual computer, a plethora of harmful virus files was found on the internet to conduct performance tests on various antivirus programs. As demonstrated in Figure 3 a total of 17 deleterious viruses were discovered, which could be categorized as either strong or weak harmful viruses. All types of harmful viruses were utilized to ensure that the antivirus programs were capable of handling any potential threat that their users may encounter.



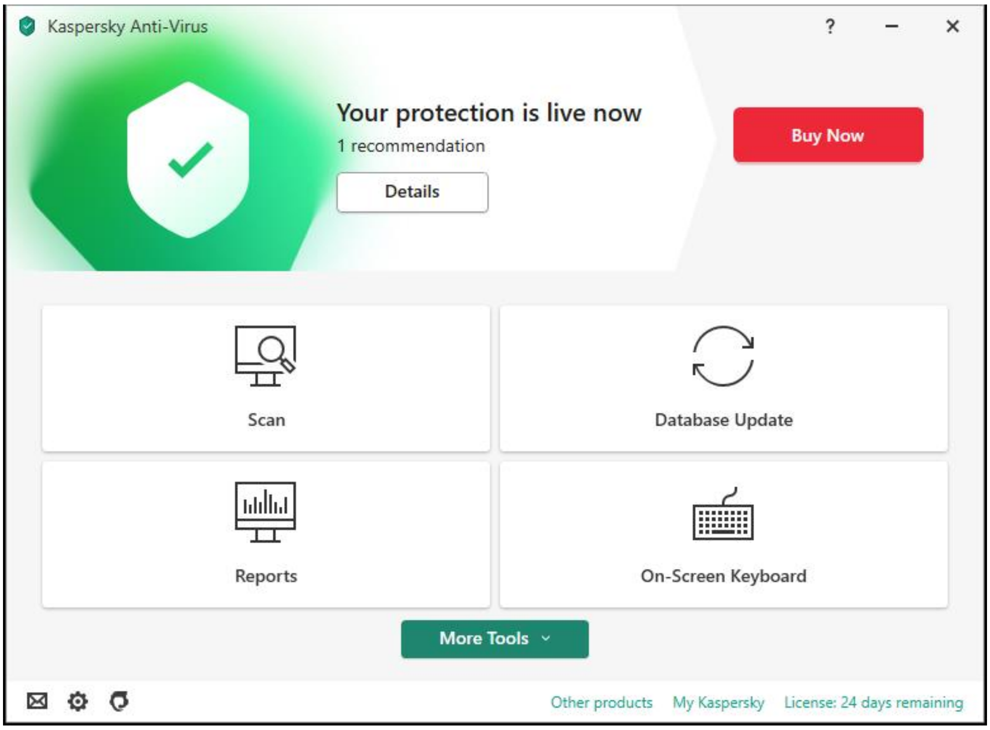
Name	Date modified	Type	Size
auto_SettingContent-ms-master	2/11/2023 7:49 PM	File folder	
cors-poc-master	2/11/2023 7:49 PM	File folder	
CrackMapExec-master	2/11/2023 7:49 PM	File folder	
cve-2019-19781-master	2/11/2023 7:49 PM	File folder	
hash_parser-master	2/11/2023 7:49 PM	File folder	
HoneyBadger-master	2/11/2023 7:49 PM	File folder	
inProc_Evade_Get-InjectedThread-master	2/11/2023 7:49 PM	File folder	
metasploit-framework-master	2/11/2023 7:49 PM	File folder	
meterssh-master	2/11/2023 7:49 PM	File folder	
nps_payload-master	2/11/2023 7:49 PM	File folder	
physical-docs-master	2/11/2023 7:49 PM	File folder	
pivoter-master	2/11/2023 7:49 PM	File folder	
Responder-master	2/11/2023 7:49 PM	File folder	
SHIPS-master	2/11/2023 7:49 PM	File folder	
SimplyEmail-master	2/11/2023 7:49 PM	File folder	
spraywmi-master	2/11/2023 7:49 PM	File folder	
wpupdate-master	2/11/2023 7:49 PM	File folder	
auto_SettingContent-ms-master	2/11/2023 7:46 PM	WinRAR ZIP archive	4 KB
cors-poc-master	2/11/2023 7:50 PM	WinRAR ZIP archive	3 KB
CrackMapExec-master	2/11/2023 7:47 PM	WinRAR ZIP archive	72 KB
cve-2019-19781-master	2/11/2023 7:46 PM	WinRAR ZIP archive	10 KB
hash_parser-master	2/11/2023 7:47 PM	WinRAR ZIP archive	2 KB
HoneyBadger-master	2/11/2023 7:46 PM	WinRAR ZIP archive	255 KB
inProc_Evade_Get-InjectedThread-master	2/11/2023 7:46 PM	WinRAR ZIP archive	15 KB
metasploit-framework-master	2/11/2023 7:47 PM	WinRAR ZIP archive	41,672 KB
meterssh-master	2/11/2023 7:47 PM	WinRAR ZIP archive	8 KB
nps_payload-master	2/11/2023 7:47 PM	WinRAR ZIP archive	7 KB
physical-docs-master	2/11/2023 7:46 PM	WinRAR ZIP archive	6 KB
pivoter-master	2/11/2023 7:47 PM	WinRAR ZIP archive	81 KB
Responder-master	2/11/2023 7:47 PM	WinRAR ZIP archive	158 KB
SHIPS-master	2/11/2023 7:47 PM	WinRAR ZIP archive	631 KB
SimplyEmail-master	2/11/2023 7:47 PM	WinRAR ZIP archive	99 KB
spraywmi-master	2/11/2023 7:47 PM	WinRAR ZIP archive	1,790 KB
wpupdate-master	2/11/2023 7:47 PM	WinRAR ZIP archive	8 KB

Figure 3: Malicious Virus Table Found

4.3 Kaspersky Antivirus Performance Test

4.3.1 Introduction about the main page

The performance test included the Kaspersky antivirus program. As seen in Figure 4, upon launching the program, it was observed that the antivirus software was either up-to-date or required an update, which was subsequently carried out. Following this, we proceeded to test the harmful viruses we had previously found individually within the Kaspersky antivirus program. The results clearly indicated that Kaspersky antivirus has an easily comprehensible and prominent user interface.



Your protection is live now

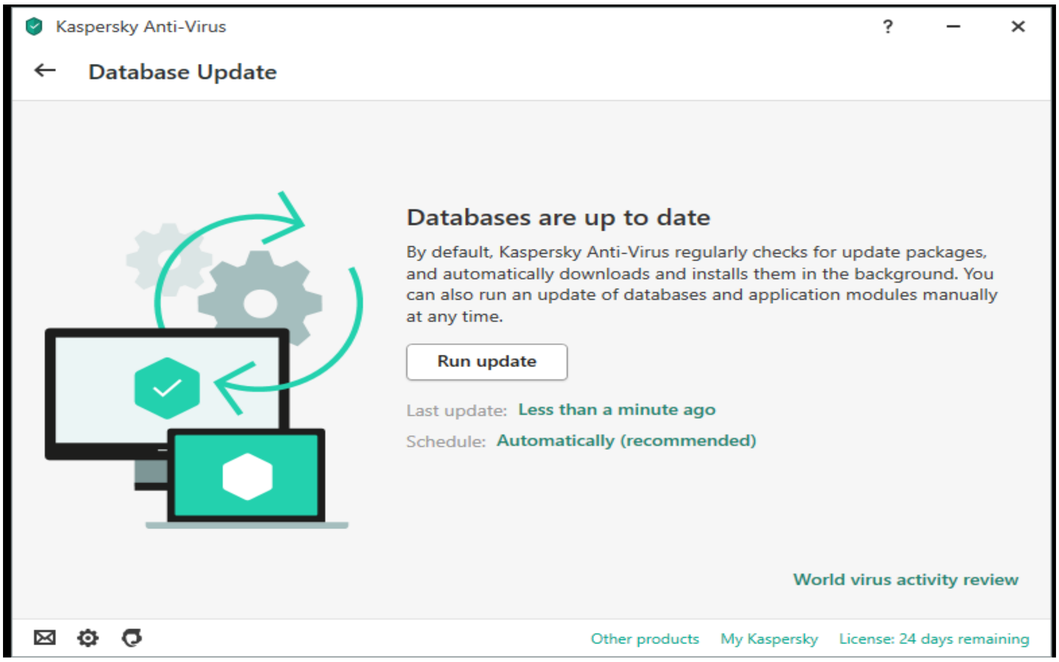
1 recommendation

License: 24 days remaining

Figure 4: Kaspersky Antivirus Software Main Page

4.3.2 Kaspersky Update check

Upon downloading the Kaspersky antivirus program, it was noted that the "Database Update" section was prominently displayed in the middle of the main page. This made it easy to determine whether the downloaded antivirus program was up-to-date. As you can see the Figure 5 as the program had just been downloaded, it was not up-to-date, and so the latest version was downloaded to prepare the system for scanning. Once the system was ready for scanning, the computer scanning process was initiated.



Databases are up to date

By default, Kaspersky Anti-Virus regularly checks for update packages, and automatically downloads and installs them in the background. You can also run an update of databases and application modules manually at any time.

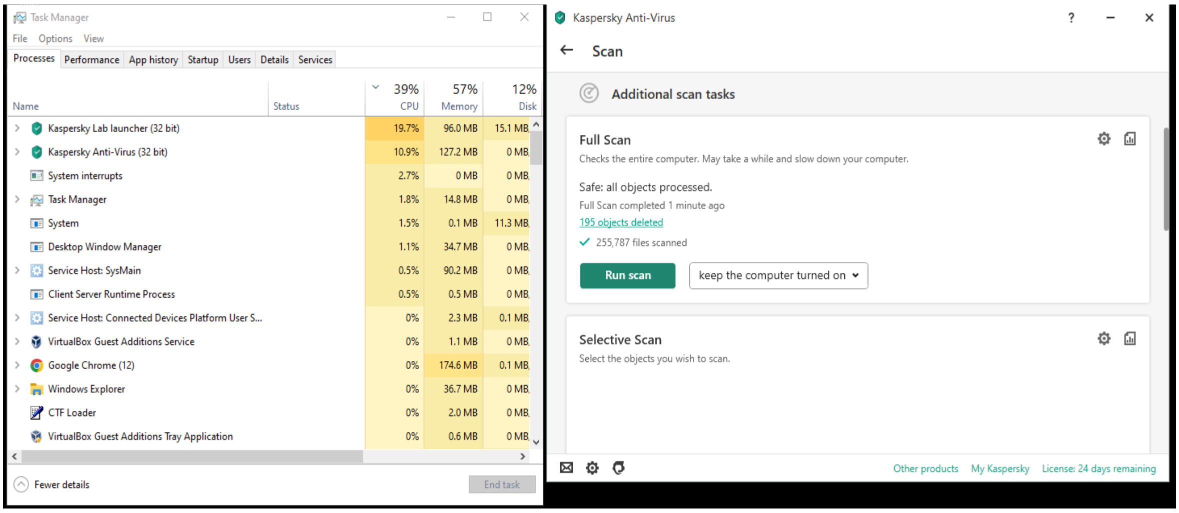
Last update: Less than a minute ago

Schedule: Automatically (recommended)

Figure 5: Kaspersky Antivirus Software Update Check page

4.3.3 Kaspersky Performance Test Result

Following the update, a scan was initiated as shown in the previous section. During the scan, the Kaspersky antivirus program was able to identify and delete a total of 255787 files, including 195 harmful viruses, which were deemed potentially harmful to the computer. During the scanning process, the program consumed a significant amount of CPU resources, reaching %98.6 usage, which was sustained until the end of the scanning process. After completion, it can been Figure 6 the CPU usage decreased to %19.7. As for the memory usage, it was observed that the program utilized a total of 223.2 MB and %57 Mermory.



Name	Status	39% CPU	57% Memory	12% Disk
Kaspersky Lab launcher (32 bit)		19.7%	96.0 MB	15.1 MB,
Kaspersky Anti-Virus (32 bit)		10.9%	127.2 MB	0 MB,
System interrupts		2.7%	0 MB	0 MB,
Task Manager		1.8%	14.8 MB	0 MB,
System		1.5%	0.1 MB	11.3 MB,
Desktop Window Manager		1.1%	34.7 MB	0 MB,
Service Host: SysMain		0.5%	90.2 MB	0 MB,
Client Server Runtime Process		0.5%	0.5 MB	0 MB,
Service Host: Connected Devices Platform User S...		0%	2.3 MB	0.1 MB,
VirtualBox Guest Additions Service		0%	1.1 MB	0 MB,
Google Chrome (12)		0%	174.6 MB	0.1 MB,
Windows Explorer		0%	36.7 MB	0 MB,
CTF Loader		0%	2.0 MB	0 MB,
VirtualBox Guest Additions Tray Application		0%	0.6 MB	0 MB,

Additional scan tasks

Full Scan

Checks the entire computer. May take a while and slow down your computer.

Safe: all objects processed.

Full Scan completed 1 minute ago

195 objects deleted

✓ 255,787 files scanned

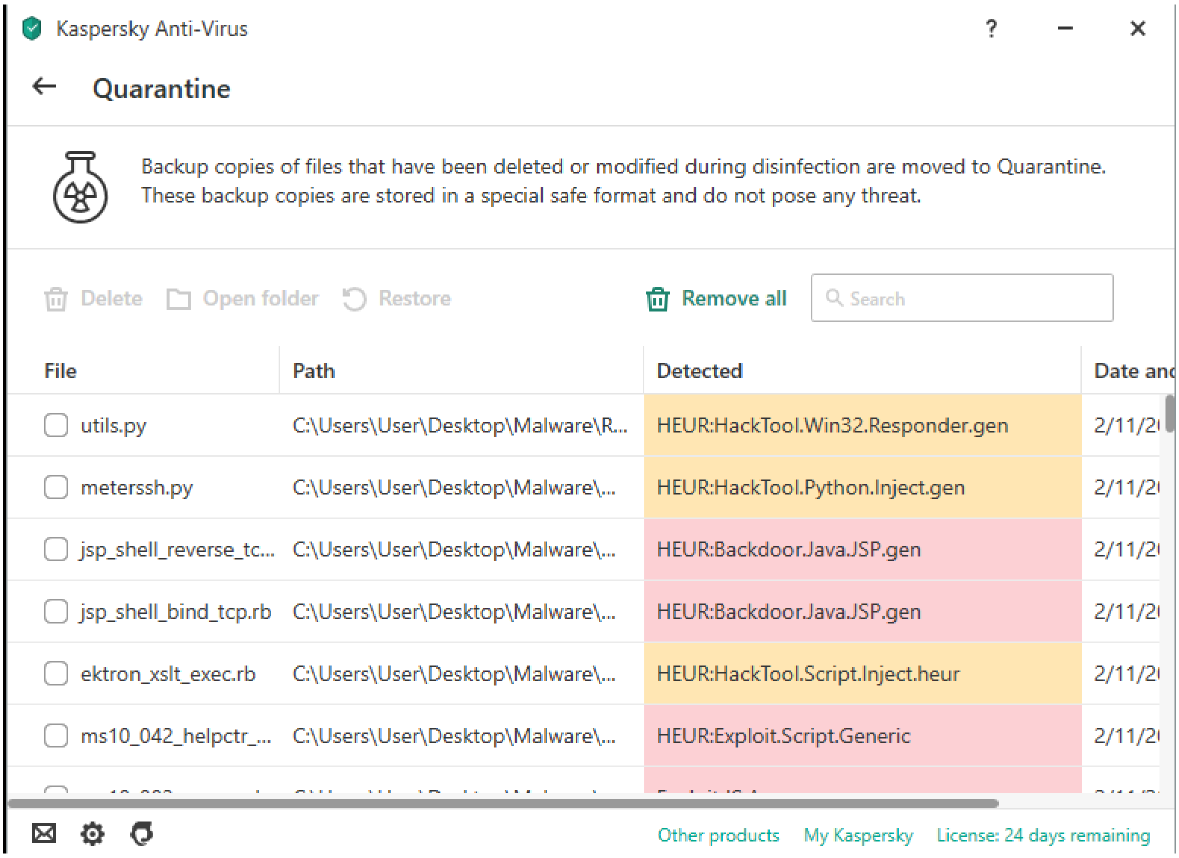
Selective Scan

Select the objects you wish to scan.

Figure 6: Kaspersky Antivirus Software Performance Result

4.3.4 Analysis of malicious virus found

After the scanning process is completed and after finding and deleting some harmful files and harmful viruses, the remaining harmful viruses that it considers dangerous are shows in Figure 7. This antivirus program can delete the files or harmful viruses that it deems detrimental to this computer and quarantine, it upon the user's request, or it can keep it under quarantine in a way that does not harm the computer.



Backup copies of files that have been deleted or modified during disinfection are moved to Quarantine. These backup copies are stored in a special safe format and do not pose any threat.

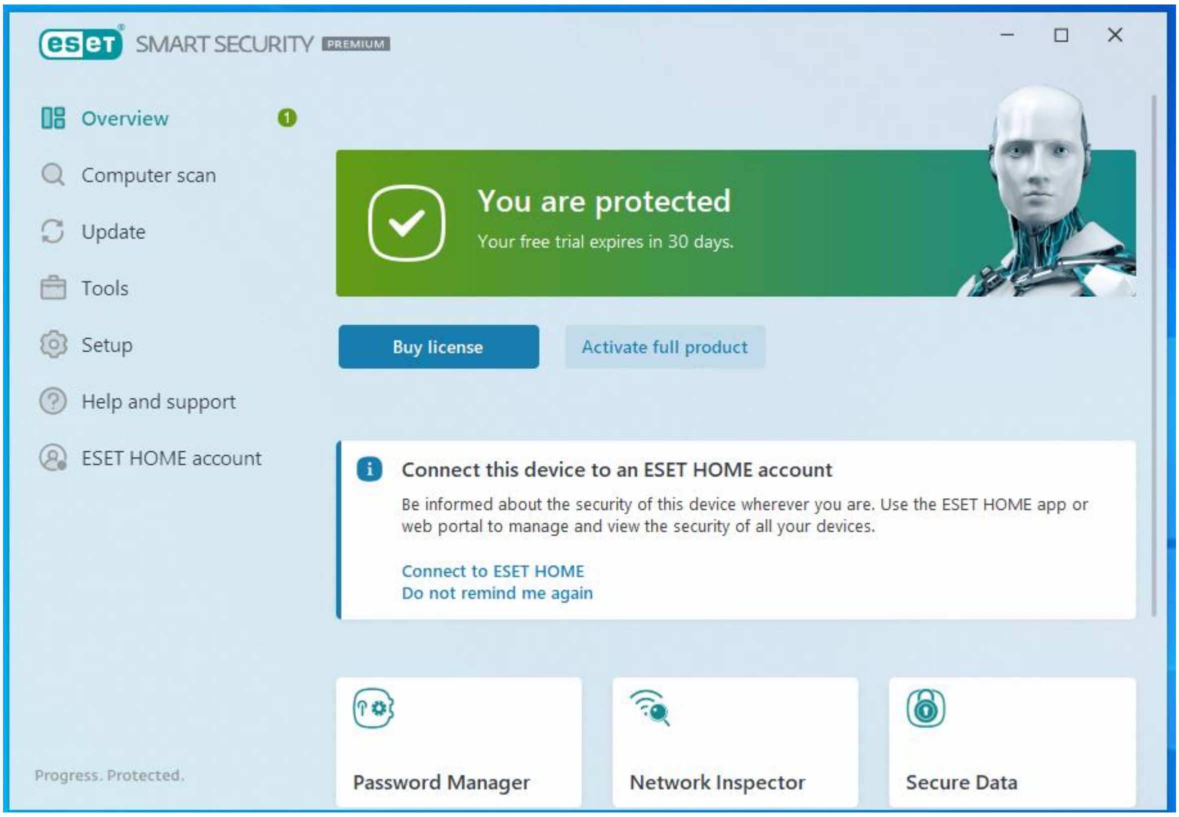
File	Path	Detected	Date and
□ utils.py	C:\Users\User\Desktop\Malware\R...	HEUR:HackTool.Win32.Responder.gen	2/11/2
□ meterssh.py	C:\Users\User\Desktop\Malware\...	HEUR:HackTool.Python.Inject.gen	2/11/2
□ jsp_shell_reverse_tc...	C:\Users\User\Desktop\Malware\...	HEUR:Backdoor.Java.JSP.gen	2/11/2
□ jsp_shell_bind_tcp.rb	C:\Users\User\Desktop\Malware\...	HEUR:Backdoor.Java.JSP.gen	2/11/2
□ ektron_xslt_exec.rb	C:\Users\User\Desktop\Malware\...	HEUR:HackTool.Script.Inject.heur	2/11/2
□ ms10_042_helpctr_...	C:\Users\User\Desktop\Malware\...	HEUR:Exploit.Script.Generic	2/11/2

Figure 7: Kaspersky Antivirus Software Virus Quarantine Page

4.4 ESET Antivirus Performance Test

4.4.1 Introduction about main page

As mentioned earlier, we conducted a performance test on the ESET antivirus program. As shown in the Figure 8, ESET's user interface is intuitive and straightforward, Figure 8 can be seen the making it accessible to users who may have little or no prior experience with antivirus programs. This feature of the program is particularly helpful for those who may not have a technical background but still need reliable antivirus protection for their computer systems.



You are protected

Your free trial expires in 30 days.

Connect this device to an ESET HOME account

Be informed about the security of this device wherever you are. Use the ESET HOME app or web portal to manage and view the security of all your devices.

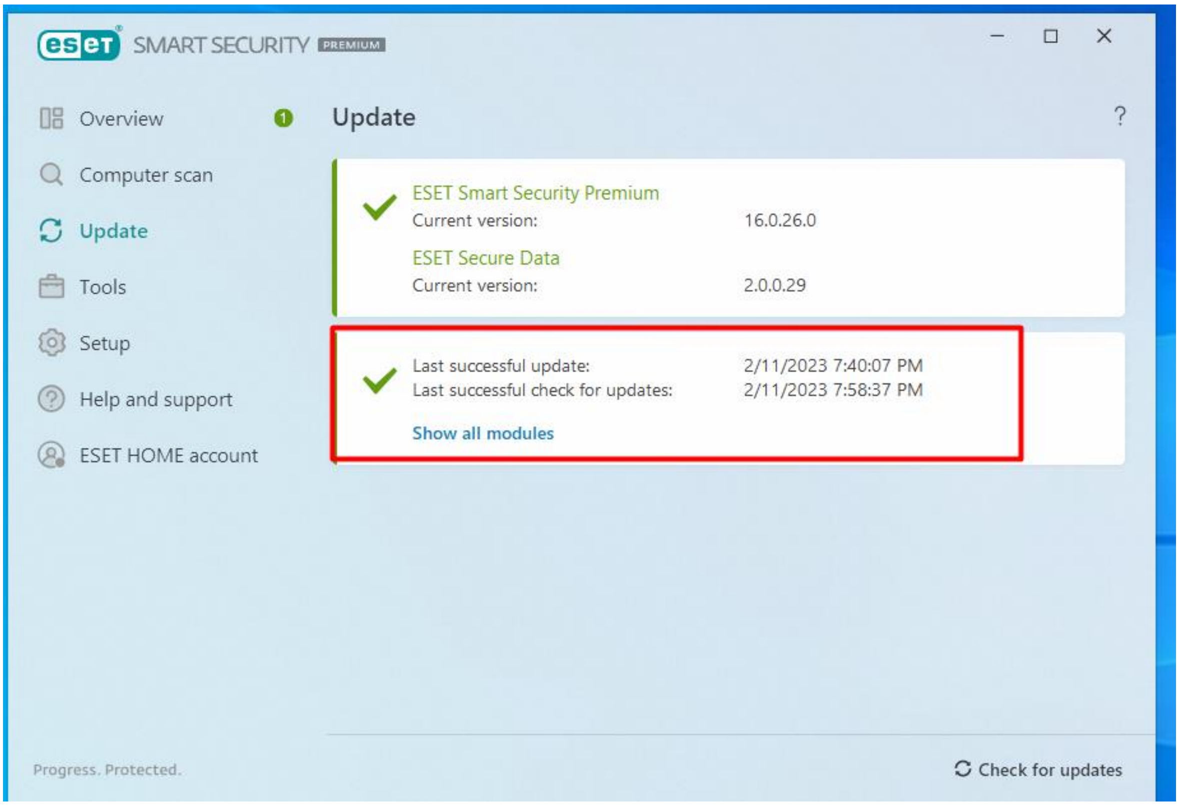
Connect to ESET HOME

Do not remind me again

Figure 8: ESET Antivirus Software Home Page

4.4.2 ESET Antivirus Update control

Upon downloading and running the ESET antivirus program, the main page displayed as shown in the Figure 9. Clicking on the "Update" section of the main page prompted the program to check for updates, which revealed that the antivirus program was out of date and needed to be updated. After the Figure 9 update, the program automatically displayed a warning message indicating that the system was up-to-date and that it was "Ready for scanning." This feature ensures that the program is always up-to-date and ready to detect any potential threats to the user's computer system.



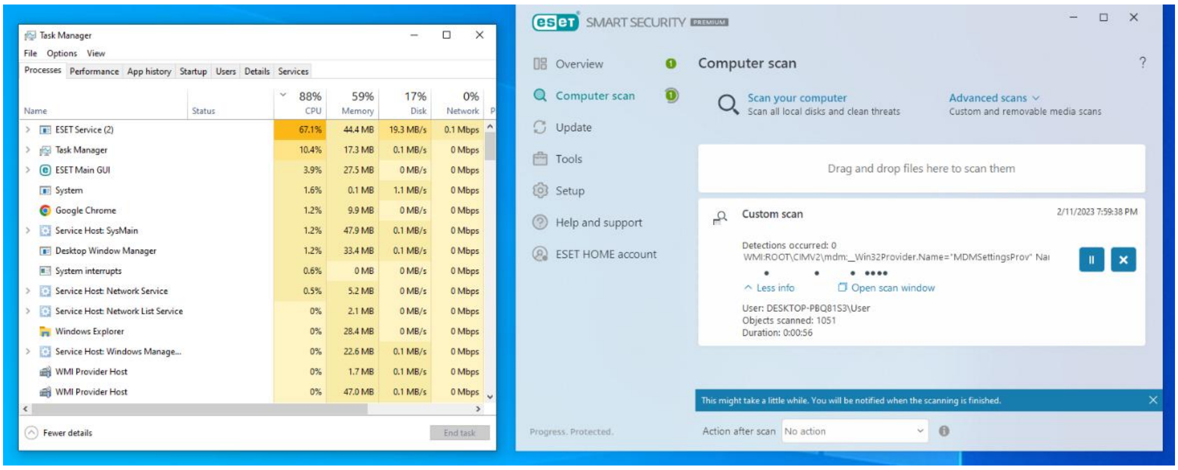
ESET Smart Security Premium
Current version: 16.0.26.0
ESET Secure Data
Current version: 2.0.0.29

Last successful update: 2/11/2023 7:40:07 PM
Last successful check for updates: 2/11/2023 7:58:37 PM

Figure 9: ESET Antivirus Software Update Page

4.4.3 ESET Performance Test Result

Upon completing the setup process for the ESET antivirus program on our virtual computer, we proceeded to initiate a scan of the system for harmful viruses. As depicted in the Figure 10, the program performed exceptionally well in comparison to other antivirus programs, using only %9.5 CPU and %73.6 memory resources. Figure 11 shows that the scan results showed that ESET successfully identified and isolated a total of 26734 harmful files and viruses, out of which it directly deleted 124 of them.This outcome is a testament to the effectiveness and efficiency of ESET in protecting computers against malicious threats.



Name	Status	88% CPU	59% Memory	17% Disk	0% Network
ESET Service (2)		67.1%	44.4 MB	19.3 MB/s	0.1 Mbps
Task Manager		10.4%	17.3 MB	0.1 MB/s	0 Mbps
ESET Main GUI		3.9%	27.5 MB	0 MB/s	0 Mbps
System		1.6%	0.1 MB	1.1 MB/s	0 Mbps
Google Chrome		1.2%	9.9 MB	0 MB/s	0 Mbps
Service Host: SysMain		1.2%	47.9 MB	0.1 MB/s	0 Mbps
Desktop Window Manager		1.2%	33.4 MB	0.1 MB/s	0 Mbps
System interrupts		0.6%	0 MB	0 MB/s	0 Mbps
Service Host: Network Service		0.5%	5.2 MB	0 MB/s	0 Mbps
Service Host: Network List Service		0%	2.1 MB	0 MB/s	0 Mbps
Windows Explorer		0%	28.4 MB	0 MB/s	0 Mbps
Service Host: Windows Manage...		0%	22.6 MB	0.1 MB/s	0 Mbps
WMI Provider Host		0%	1.7 MB	0.1 MB/s	0 Mbps
WMI Provider Host		0%	47.0 MB	0.1 MB/s	0 Mbps

Computer scan

Scan your computer
Scan all local disks and clean threats

Advanced scans
Custom and removable media scans

Drag and drop files here to scan them

Custom scan 2/11/2023 7:59:38 PM

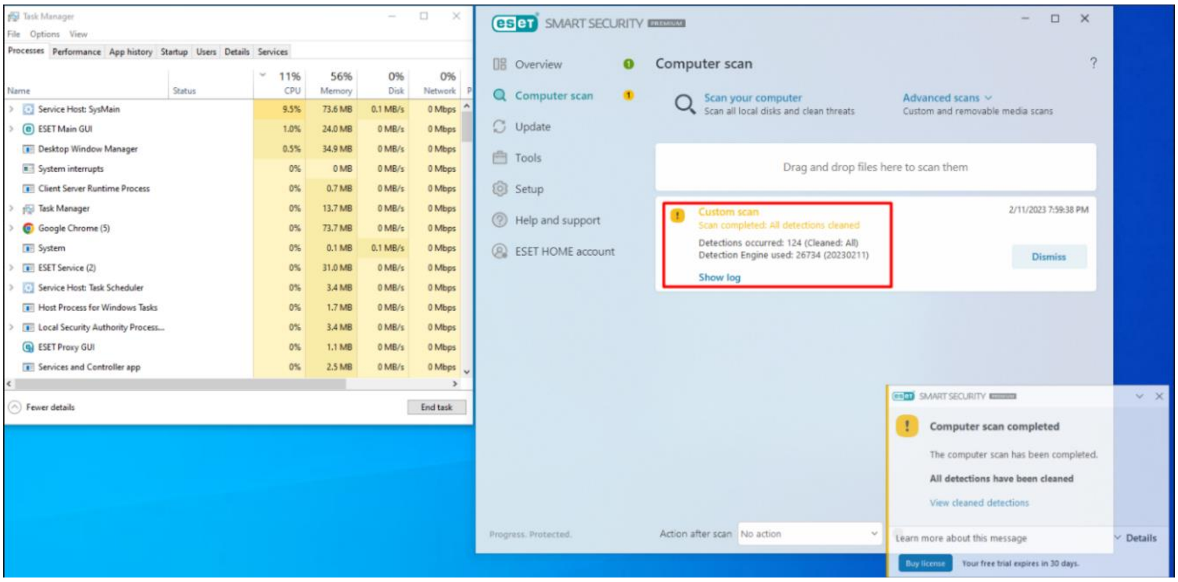
Detections occurred: 0
WMI:ROOT\CIMV2\mdm:_Win32Provider.Name="MDMSettingsProv" Nai

User: DESKTOP-PBQ81S3\User
Objects scanned: 1051
Duration: 0:00:56

This might take a little while. You will be notified when the scanning is finished.

Action after scan: No action

Figure 10: ESET Antivirus Software Computer Scan Page



Name	Status	11% CPU	56% Memory	0% Disk	0% Network
Service Host: SysMain		9.5%	73.6 MB	0.1 MB/s	0 Mbps
ESET Main GUI		1.0%	24.0 MB	0 MB/s	0 Mbps
Desktop Window Manager		0.5%	34.9 MB	0 MB/s	0 Mbps
System interrupts		0%	0 MB	0 MB/s	0 Mbps
Client Server Runtime Process		0%	0.7 MB	0 MB/s	0 Mbps
Task Manager		0%	13.7 MB	0 MB/s	0 Mbps
Google Chrome (5)		0%	73.7 MB	0 MB/s	0 Mbps
System		0%	0.1 MB	0.1 MB/s	0 Mbps
ESET Service (2)		0%	31.0 MB	0 MB/s	0 Mbps
Service Host: Task Scheduler		0%	3.4 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	1.7 MB	0 MB/s	0 Mbps
Local Security Authority Process...		0%	3.4 MB	0 MB/s	0 Mbps
ESET Proxy GUI		0%	1.1 MB	0 MB/s	0 Mbps
Services and Controller app		0%	2.5 MB	0 MB/s	0 Mbps

Computer scan

Scan your computer
Scan all local disks and clean threats

Advanced scans
Custom and removable media scans

Drag and drop files here to scan them

Custom scan 2/11/2023 7:59:38 PM
Scan completed: All detections cleaned
Detections occurred: 124 (Cleaned: All)
Detection Engine used: 26734 (20230211)

Action after scan: No action

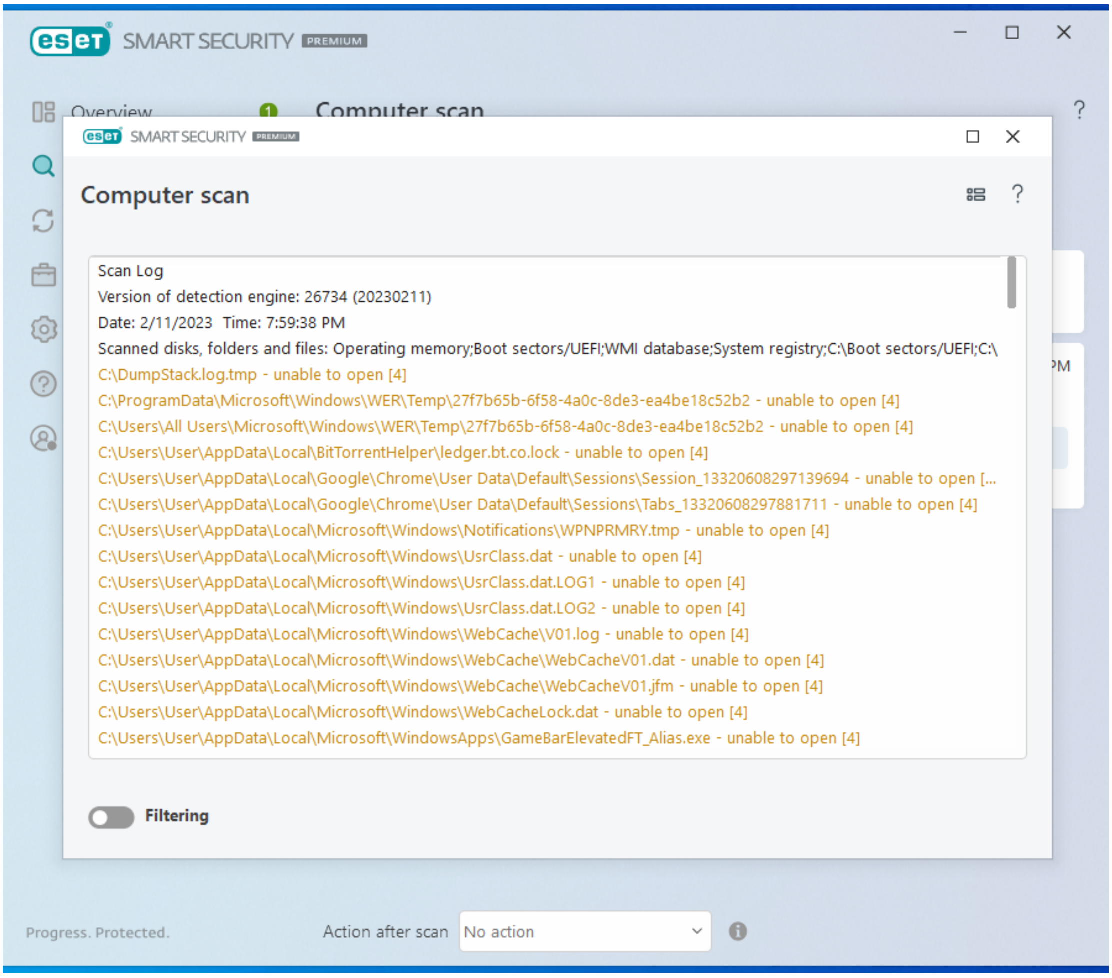
Computer scan completed
The computer scan has been completed.
All detections have been cleaned

Your free trial expires in 30 days.

Figure 11: ESET Antivirus Software Performance Result

4.4.4 Malicious virus analysis

Figure 12, the ESET antivirus program successfully detected 26734 malicious files during the scanning test. These files are capable of causing harm to the computer and its security. Figure 12 shows that the total number of files scanned during the test was 20230211. ESET's ability to detect and remove harmful files ensures the protection and security of the user's computer.



```
Scan Log
Version of detection engine: 26734 (20230211)
Date: 2/11/2023  Time: 7:59:38 PM
Scanned disks, folders and files: Operating memory;Boot sectors/UEFI;WMI database;System registry;C:\Boot sectors/UEFI;C:\
C:\DumpStack.log.tmp - unable to open [4]
C:\ProgramData\Microsoft\Windows\WER\Temp\27f7b65b-6f58-4a0c-8de3-ea4be18c52b2 - unable to open [4]
C:\Users\All Users\Microsoft\Windows\WER\Temp\27f7b65b-6f58-4a0c-8de3-ea4be18c52b2 - unable to open [4]
C:\Users\User\AppData\Local\BitTorrentHelper\ledger.bt.co.lock - unable to open [4]
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Sessions\Session_13320608297139694 - unable to open [...
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Sessions\Tabs_13320608297881711 - unable to open [4]
C:\Users\User\AppData\Local\Microsoft\Windows\Notifications\WPNPRMRY.tmp - unable to open [4]
C:\Users\User\AppData\Local\Microsoft\Windows\UsrClass.dat - unable to open [4]
C:\Users\User\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1 - unable to open [4]
C:\Users\User\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2 - unable to open [4]
C:\Users\User\AppData\Local\Microsoft\Windows\WebCache\V01.log - unable to open [4]
C:\Users\User\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat - unable to open [4]
C:\Users\User\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.jfm - unable to open [4]
C:\Users\User\AppData\Local\Microsoft\Windows\WebCacheLock.dat - unable to open [4]
C:\Users\User\AppData\Local\Microsoft\WindowsApps\GameBarElevatedFT_Alias.exe - unable to open [4]
```

Filtering

Progress. Protected.

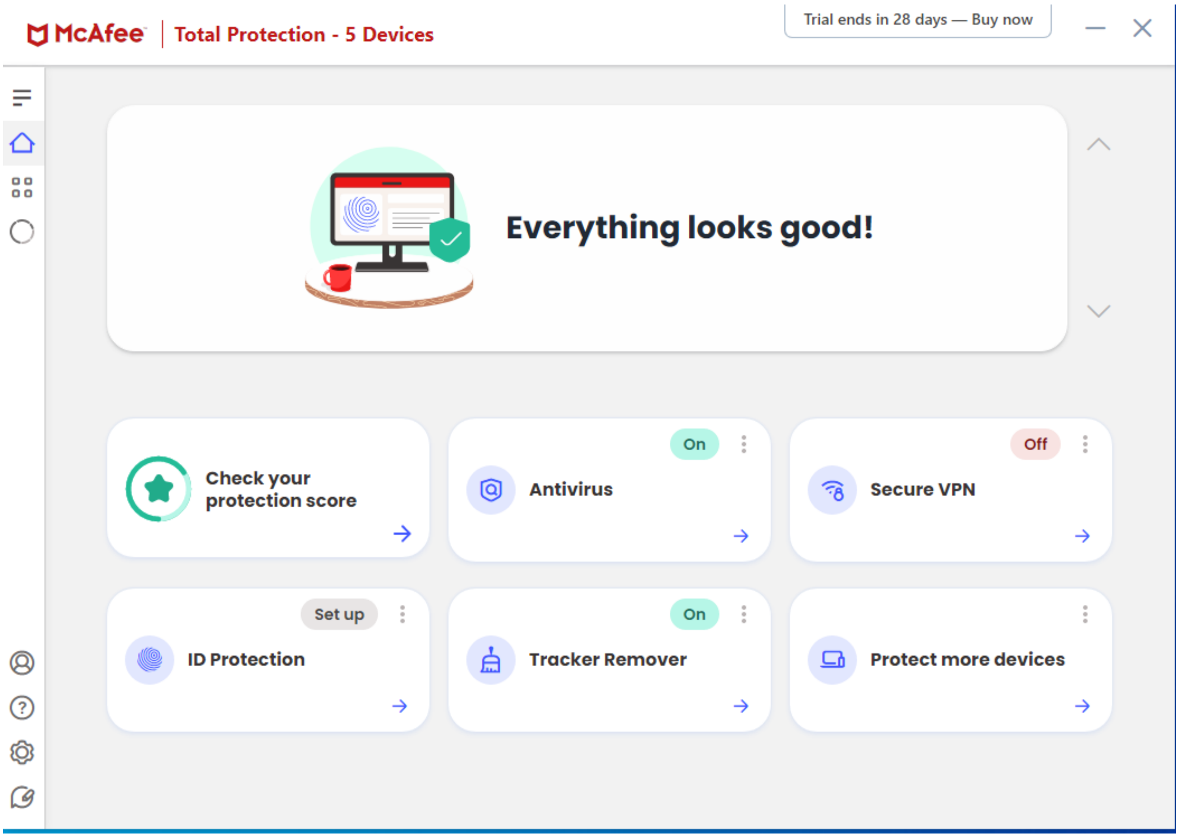
Action after scan: No action

Figure 12: ESET Antivirus Software Virus Analysis Page

4.5 McAfee Performance Test

4.5.1 Introduction about main page

Next up for testing is the McAfee antivirus program. Figure 13 demonstrates upon downloading and installing the program, the main interface of McAfee is immediately visible. Immediately after the program was run, we received a notification that the latest version should be downloaded directly from the program, and we immediately installed the latest updated version. After updating the antivirus program, we ran the harmful viruses we found individually and tested them in the McAfee antivirus program. As it can be seen in the Figure 13, the McAfee antivirus program has an apparent and understandable main face and offers a few features to provide extra computer protection.



Trial ends in 28 days — Buy now

Everything looks good!

Antivirus On

Secure VPN Off

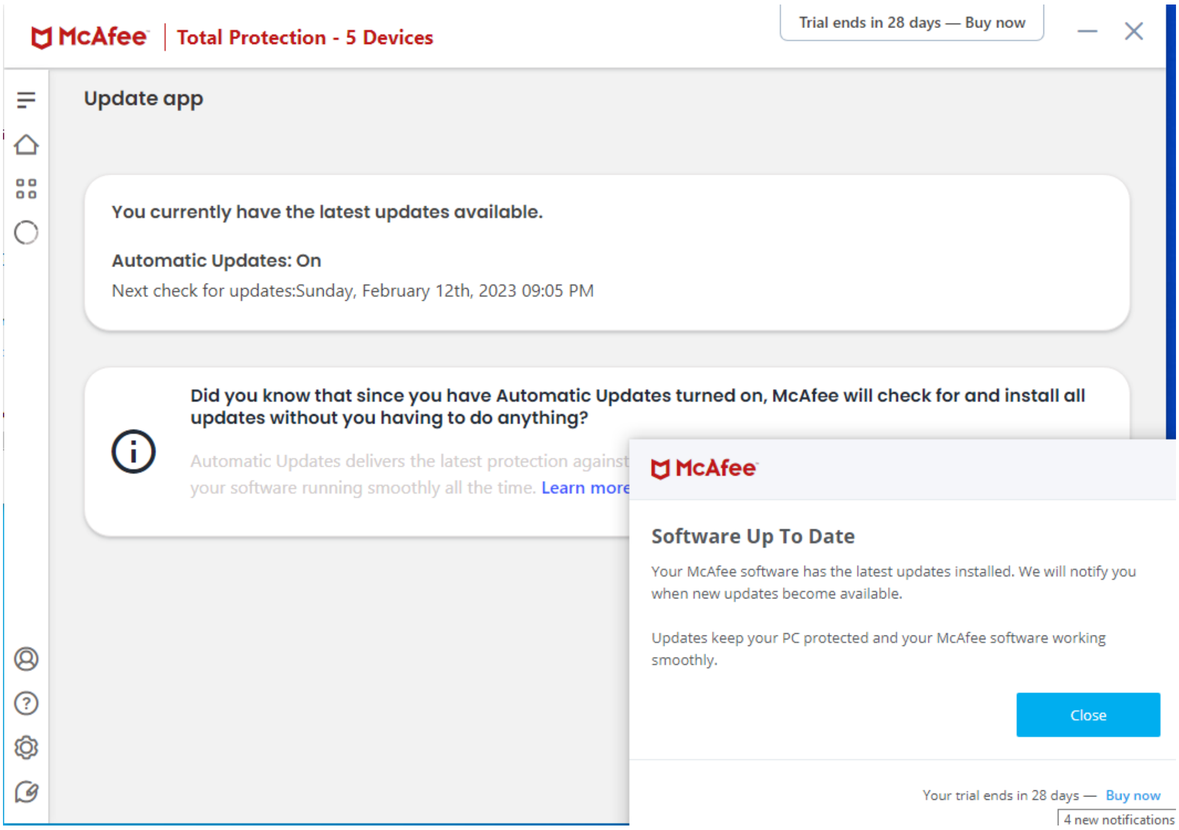
ID Protection Set up

Tracker Remover On

Figure 13: McAfee Antivirus Software Home Page

4.5.2 McAfee Update control

Figure 14 shows that is a McAfee antivirus program that we installed on a virtual computer and ready to scan but we were prompted to update the program after downloading and installing it, and Figure 15 shows that once we updated it, the program was ready for scanning. We began the scanning process to check for any harmful viruses or files that may be on the computer.



McAfee | Total Protection - 5 Devices
Trial ends in 28 days — Buy now

Update app

You currently have the latest updates available.

Automatic Updates: On
Next check for updates:Sunday, February 12th, 2023 09:05 PM

Did you know that since you have Automatic Updates turned on, McAfee will check for and install all updates without you having to do anything?

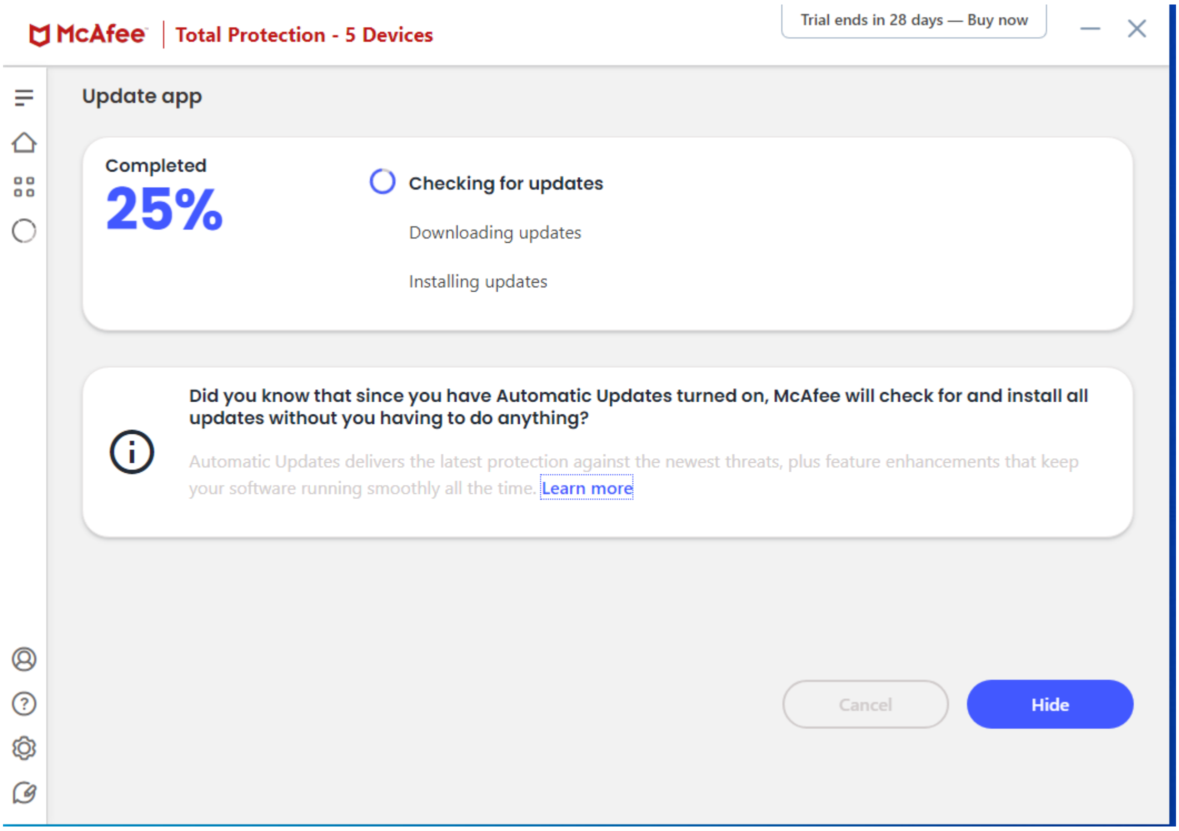
Automatic Updates delivers the latest protection against your software running smoothly all the time. Learn more

Software Up To Date

Your McAfee software has the latest updates installed. We will notify you when new updates become available.

Updates keep your PC protected and your McAfee software working smoothly.

Figure 14: McAfee Antivirus Software Notification For Update Page



Update app

Completed

25%

Checking for updates

Downloading updates

Installing updates

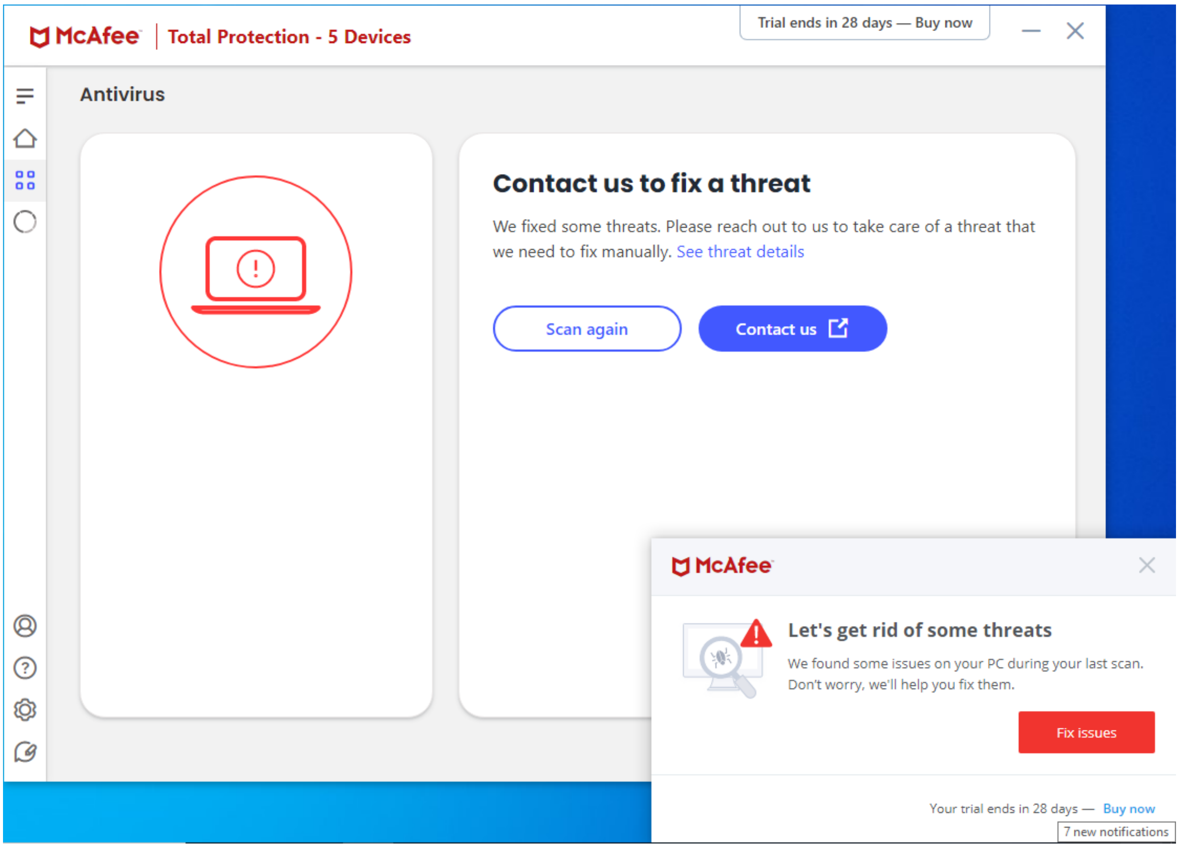
Did you know that since you have Automatic Updates turned on, McAfee will check for and install all updates without you having to do anything?

Automatic Updates delivers the latest protection against the newest threats, plus feature enhancements that keep your software running smoothly all the time. Learn more

Figure 15: McAfee Antivirus Software Update Pages

4.5.3 McAfee Scan result and Performance test result

In the performance test shown in Figure 17, the McAfee antivirus program was ready for scanning immediately after the update. It's obvious that in Figure 17. During the scanning process, the program used %76.8 CPU usage and %217.2 memory compared to other antivirus programs, which was acceptable. After the scan was completed, the McAfee antivirus program detected a total of 2428 harmful files and viruses. However, it can be seen in Figure 16 that a serious threat with the name "Important notification" was detected and a warning notification was sent to the user. Overall, the McAfee antivirus program performed well in this test.



Contact us to fix a threat

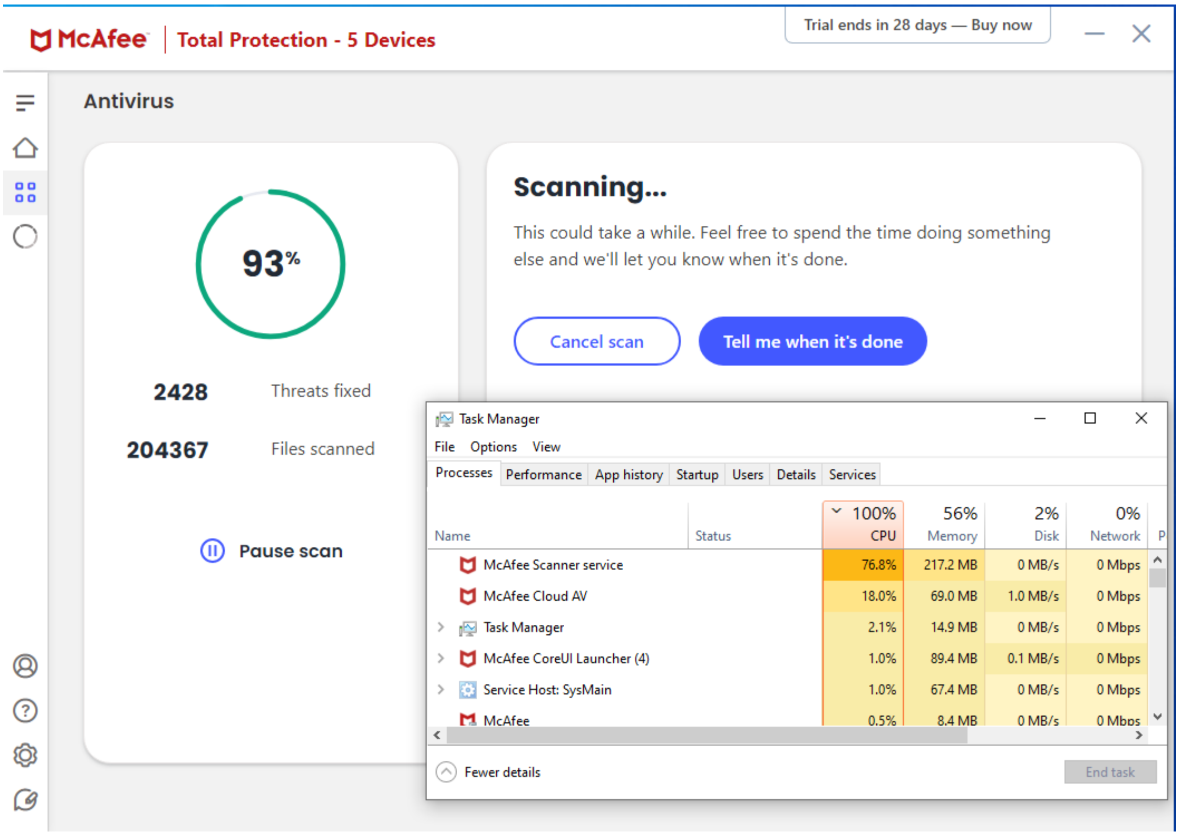
We fixed some threats. Please reach out to us to take care of a threat that we need to fix manually. See threat details

Let's get rid of some threats

We found some issues on your PC during your last scan. Don't worry, we'll help you fix them.

Your trial ends in 28 days — Buy now

Figure 16: McAfee Antivirus Software Threat Notification


McAfee
Total Protection - 5 Devices
Trial ends in 28 days — Buy now
Antivirus

93%

2428 Threats fixed

204367 Files scanned

Scanning...

This could take a while. Feel free to spend the time doing something else and we'll let you know when it's done.

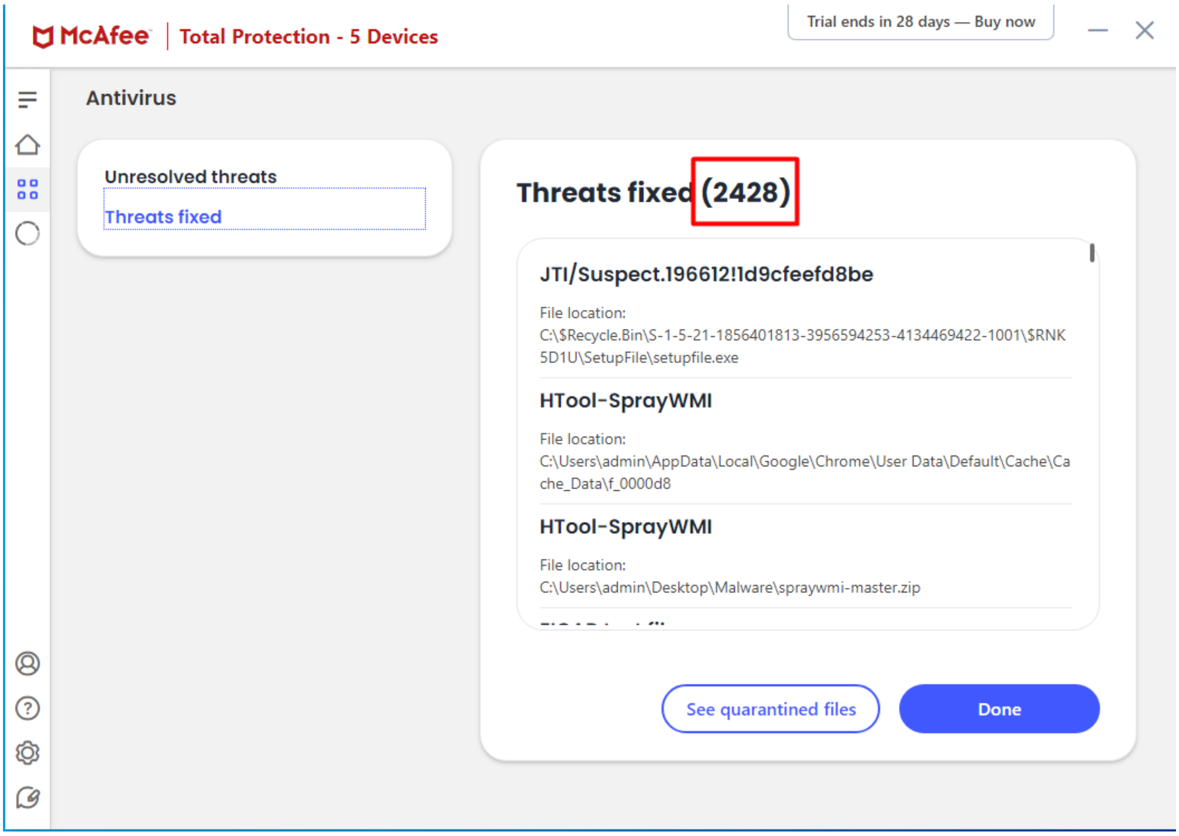
Cancel scan
Tell me when it's done
Task Manager
File Options View
Processes Performance App history Startup Users Details Services

Name	Status	100% CPU	56% Memory	2% Disk	0% Network
McAfee Scanner service		76.8%	217.2 MB	0 MB/s	0 Mbps
McAfee Cloud AV		18.0%	69.0 MB	1.0 MB/s	0 Mbps
Task Manager		2.1%	14.9 MB	0 MB/s	0 Mbps
McAfee CoreUI Launcher (4)		1.0%	89.4 MB	0.1 MB/s	0 Mbps
Service Host: SysMain		1.0%	67.4 MB	0 MB/s	0 Mbps
McAfee		0.5%	8.4 MB	0 MB/s	0 Mbps

Figure 17: McAfee Antivirus Software Performance Results

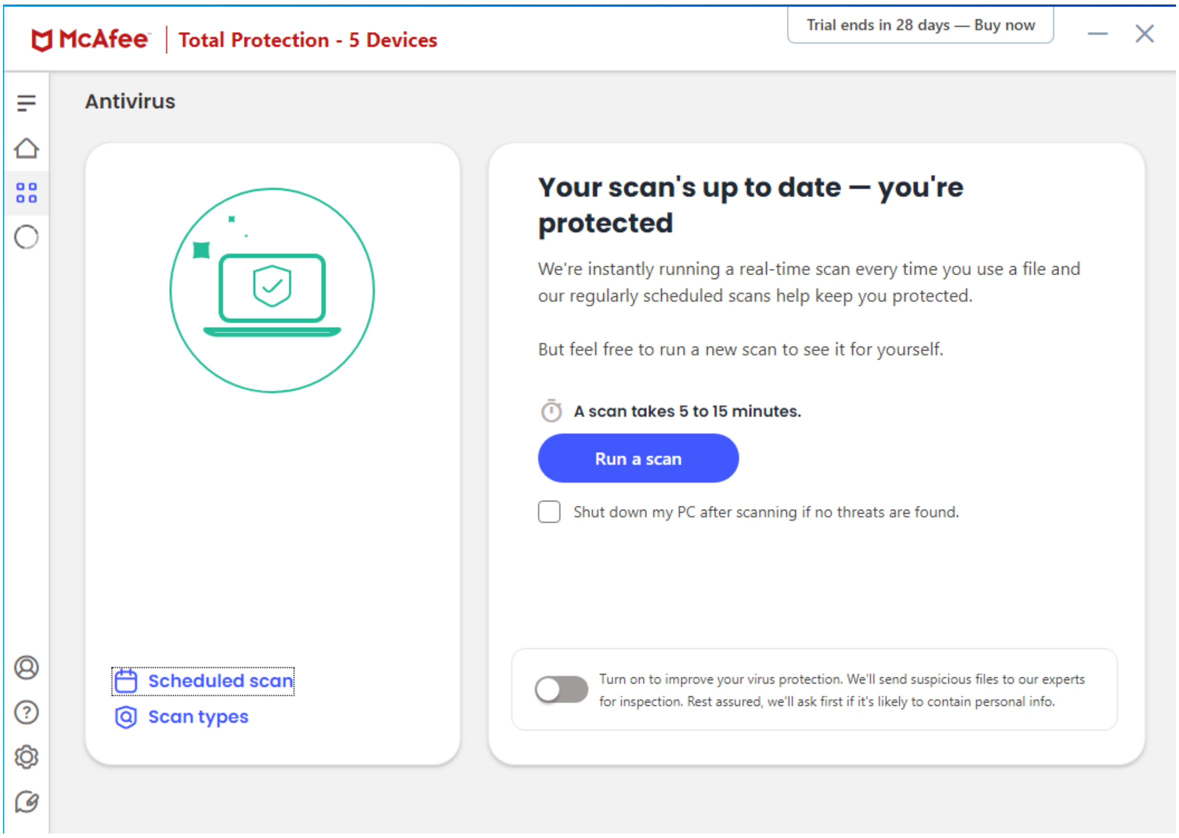
4.5.4 Malicious virus analysis

In Figure 18, the number of harmful files and viruses found after McAfee antivirus program scanning test and performance test is 2428. Figure 18 that show the total number of files and viruses that can harm the computer after 204367 scans, and Figure 19 shows that the computer has been cleaned and can be used safely.



```
JTI/Suspect.196612!1d9cfeefd8be

File location:
C:\$Recycle.Bin\S-1-5-21-1856401813-3956594253-4134469422-1001\$RNK
5D1U\SetupFile\setupfile.exe

HTool-SprayWMI

File location:
C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\Ca
che_Data\f_0000d8

HTool-SprayWMI

File location:
C:\Users\admin\Desktop\Malware\spraywmi-master.zip
```

Figure 18: McAfee Antivirus Software Threat Virus Results



McAfee | Total Protection - 5 Devices
Trial ends in 28 days — Buy now
Antivirus
Run a scan
Scheduled scan
Scan types

Your scan's up to date — you're protected

We're instantly running a real-time scan every time you use a file and our regularly scheduled scans help keep you protected.

But feel free to run a new scan to see it for yourself.

A scan takes 5 to 15 minutes.

□ Shut down my PC after scanning if no threats are found.

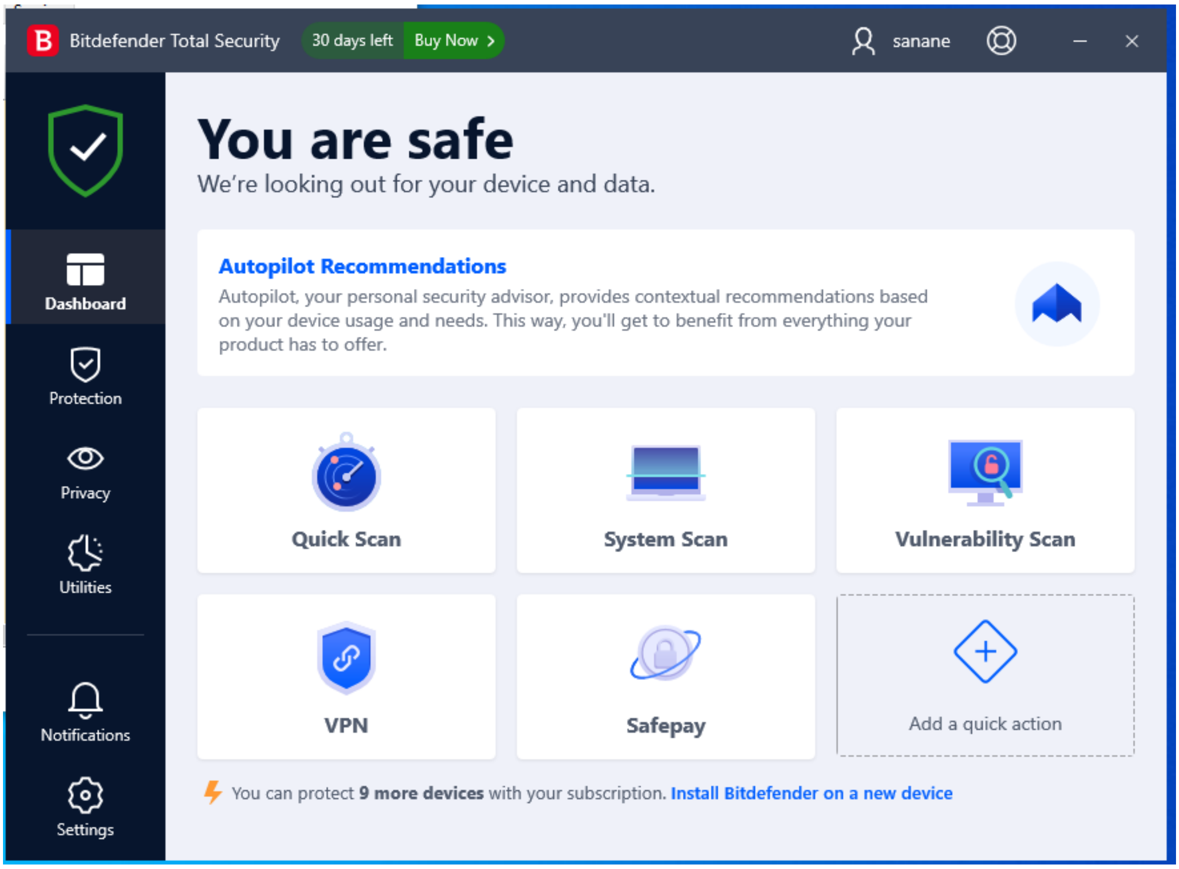
Turn on to improve your virus protection. We'll send suspicious files to our experts for inspection. Rest assured, we'll ask first if it's likely to contain personal info.

Figure 19: McAfee Antivirus Software After the General Test Result

4.6 Bitdefender Performance Test

4.6.1 Introduction about main page

As we move on to the next antivirus program, Bitdefender, we can see that its user interface is very user-friendly and easy to understand in Figure 20, even for those who have never used an antivirus program before. The main page offers various features that can be used to perform scans and improve computer security. Bitdefender is known as one of the most reliable and effective antivirus programs in the market, providing advanced protection against various types of malware, viruses, and other harmful threats.



You are safe

We're looking out for your device and data.

Autopilot Recommendations

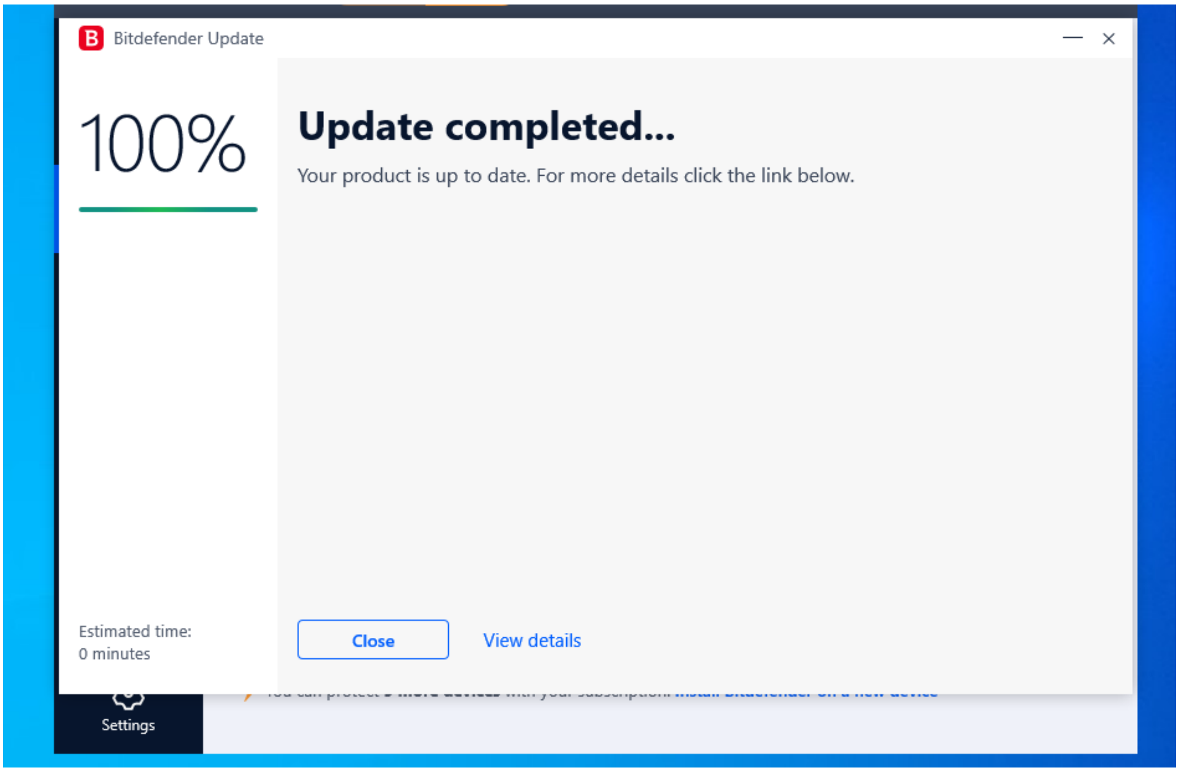
Autopilot, your personal security advisor, provides contextual recommendations based on your device usage and needs. This way, you'll get to benefit from everything your product has to offer.

You can protect **9 more devices** with your subscription. **Install Bitdefender on a new device**

Figure 20: Bitdefender Antivirus Software Main Page

4.6.2 Update check

As depicted in the Figure 21 below that after downloading and installing the Bitdefender antivirus program on the computer, the latest version update should be made on the program side like other antivirus programs. After this warning, the latest version was updated and made ready for scanning.



Update completed...

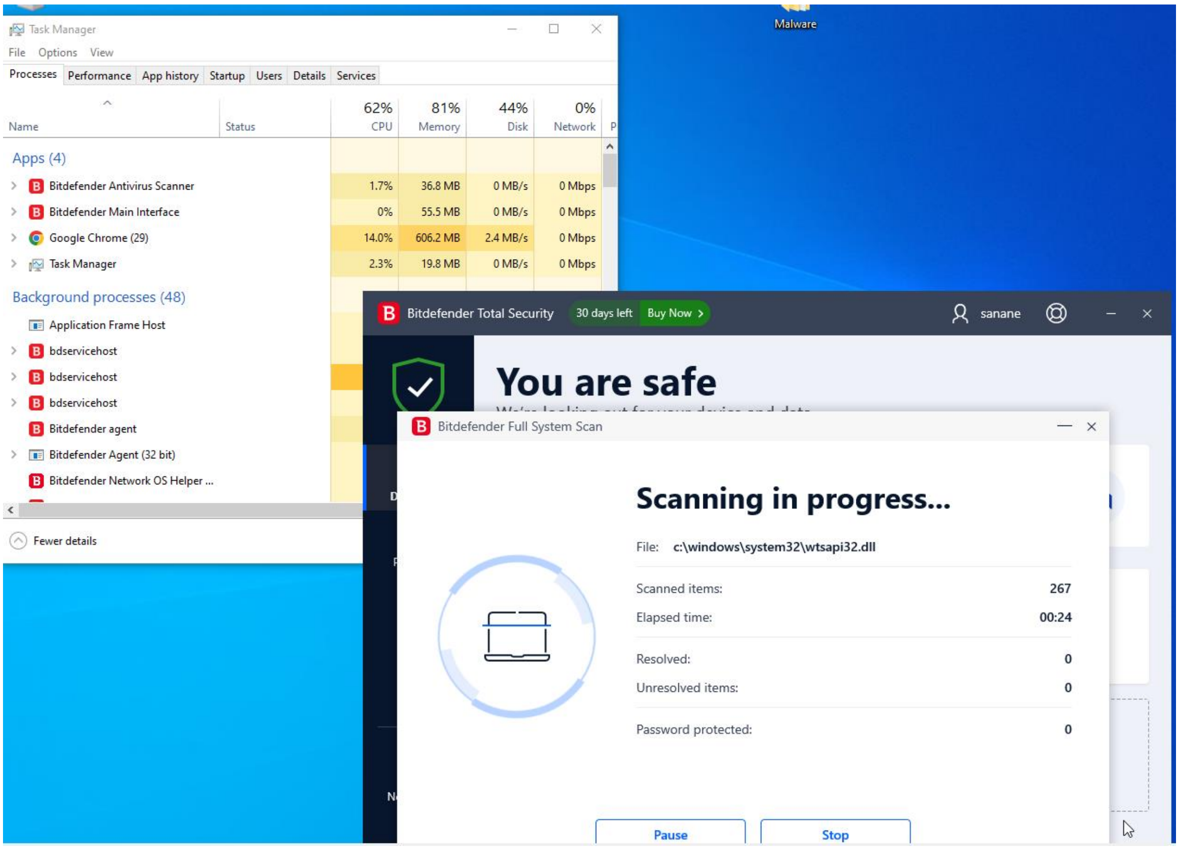
Your product is up to date. For more details click the link below.

Estimated time:
0 minutes

Figure 21: Bitdefender Antivirus Software Update Page

4.6.3 Bitdefender Scan result and Performance test

After the latest version was installed and ready by the antivirus program, we started the scanning process. As you can see in Figure 22 our results in this performance test of the Bitdefender antivirus program using % 62 CPU usage and % 81 Mermory passed this test successfully without any warning like other antivirus programs. After the malicious virus scan is finished, Figure 23 can show the number of harmful files and viruses and also it scans and finds is 418 and as seen in Figure 23, Although this result seems low compared to other antivirus programs, it is a number that can pose a severe threat to the computer.



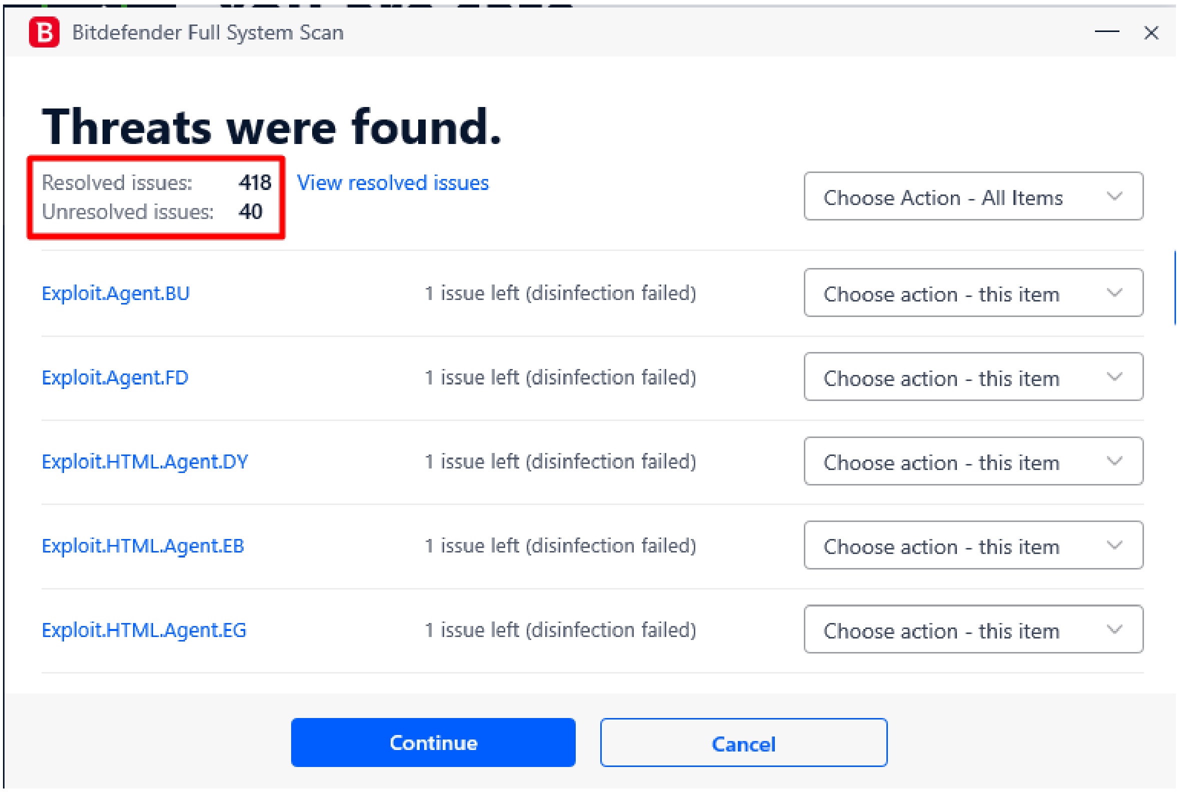
Name	Status	62% CPU	81% Memory	44% Disk	0% Network
Apps (4)					
Bitdefender Antivirus Scanner		1.7%	36.8 MB	0 MB/s	0 Mbps
Bitdefender Main Interface		0%	55.5 MB	0 MB/s	0 Mbps
Google Chrome (29)		14.0%	606.2 MB	2.4 MB/s	0 Mbps
Task Manager		2.3%	19.8 MB	0 MB/s	0 Mbps
Background processes (48)					
Application Frame Host					
bdservicehost					
bdservicehost					
bdservicehost					
Bitdefender agent					
Bitdefender Agent (32 bit)					
Bitdefender Network OS Helper ...					

Scanning in progress...

File: c:\windows\system32\wtsapi32.dll

Scanned items:	267
Elapsed time:	00:24
Resolved:	0
Unresolved items:	0
Password protected:	0

Figure 22: Bitdefender Antivirus Software Performance Test Page



Bitdefender Full System Scan

Threats were found.

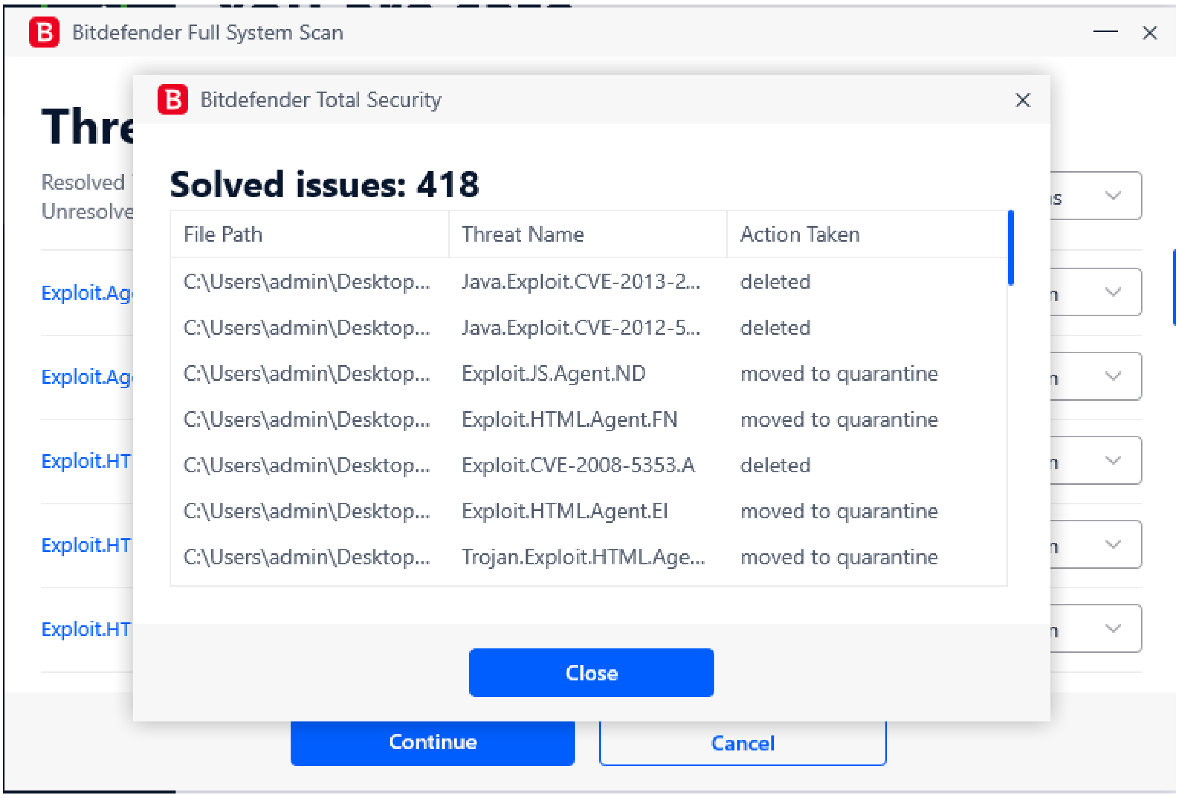
Resolved issues: 418
Unresolved issues: 40

Exploit.Agent.BU	1 issue left (disinfection failed)	Choose action - this item
Exploit.Agent.FD	1 issue left (disinfection failed)	Choose action - this item
Exploit.HTML.Agent.DY	1 issue left (disinfection failed)	Choose action - this item
Exploit.HTML.Agent.EB	1 issue left (disinfection failed)	Choose action - this item
Exploit.HTML.Agent.EG	1 issue left (disinfection failed)	Choose action - this item

Figure 23: Bitdefender Antivirus Software After the General Test Result

4.6.4 Malicious virus analysis

As shown in Figure 24 below, we have conducted a scanning and performance test on the Bitdefender antivirus program. The total number of harmful files and viruses detected by the program was 25649734 while the total number of files and viruses that could harm the computer after scanning was only 418. It is worth noting that 40 of the detected harmful viruses or files were not found to cause any problems to the computer. Overall, Bitdefender proved to be an effective antivirus program in terms of detecting harmful files and viruses, with a low number of false positives.



Solved issues: 418

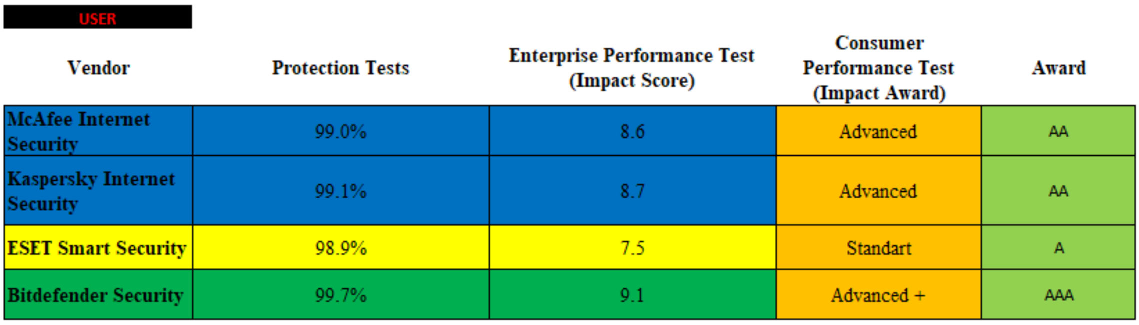
File Path	Threat Name	Action Taken
C:\Users\admin\Desktop...	Java.Exploit.CVE-2013-2...	deleted
C:\Users\admin\Desktop...	Java.Exploit.CVE-2012-5...	deleted
C:\Users\admin\Desktop...	Exploit.JS.Agent.ND	moved to quarantine
C:\Users\admin\Desktop...	Exploit.HTML.Agent.FN	moved to quarantine
C:\Users\admin\Desktop...	Exploit.CVE-2008-5353.A	deleted
C:\Users\admin\Desktop...	Exploit.HTML.Agent.EI	moved to quarantine
C:\Users\admin\Desktop...	Trojan.Exploit.HTML.Age...	moved to quarantine

Figure 24: Bitdefender Antivirus Software Virus Details Page

4.7 Performance Test Summary

The results below are given by the references received by the users by comparing the personal use of the products by considering all kinds of viruses that can harm the computer, except for malware and malicious viruses, and by comparing them between independent test organizations.

The awards given below will take the Normal products of antivirus programs and win awards annually based on 2022-2023 data. Guest products are rated only for the period in which they were tested.



USER

Vendor	Protection Tests	Enterprise Performance Test (Impact Score)	Consumer Performance Test (Impact Award)	Award
McAfee Internet Security	99.0%	8.6	Advanced	AA
Kaspersky Internet Security	99.1%	8.7	Advanced	AA
ESET Smart Security	98.9%	7.5	Standart	A
Bitdefender Security	99.7%	9.1	Advanced +	AAA

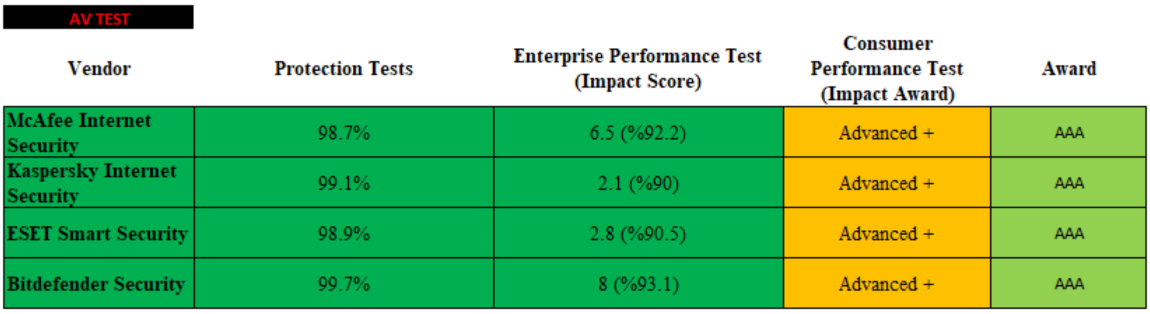
Table 2:User Survey Result Table

🟩 Advanced + 🟦 Advanced 🟨 Standart

- In the table above, awards are given using user data.
- The products tested in this report were the latest versions
- These results were obtained by taking the average of the surveys included in the user data. The main found questionnaires have been added to the reference section.

4.8 Awards

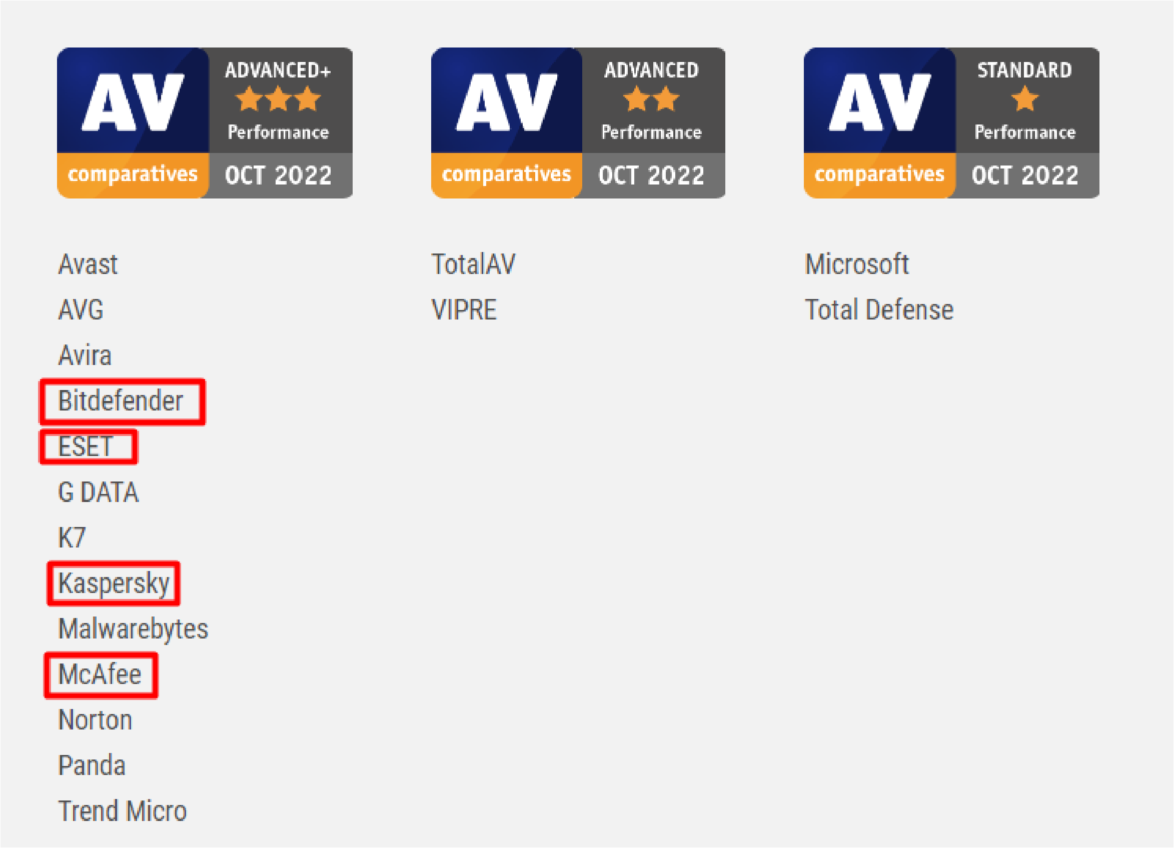
The following products win AV comparatives awards for latest performance:



AV TEST

Vendor	Protection Tests	Enterprise Performance Test (Impact Score)	Consumer Performance Test (Impact Award)	Award
McAfee Internet Security	98.7%	6.5 (%92.2)	Advanced +	AAA
Kaspersky Internet Security	99.1%	2.1 (%90)	Advanced +	AAA
ESET Smart Security	98.9%	2.8 (%90.5)	Advanced +	AAA
Bitdefender Security	99.7%	8 (%93.1)	Advanced +	AAA

Table 3:AV-Test Results Table From Excel


AV ADVANCED+ ★★★ Performance comparatives OCT 2022
AV ADVANCED ★★ Performance comparatives OCT 2022
AV STANDARD ★ Performance comparatives OCT 2022

Avast
AVG
Avira
Bitdefender
ESET
G DATA
K7
Kaspersky
Malwarebytes
McAfee
Norton
Panda
Trend Micro

TotalAV
VIPRE

Microsoft
Total Defense

Figure 25: AV Test Awards [43].

4.9 Conservation Summary Interpretation

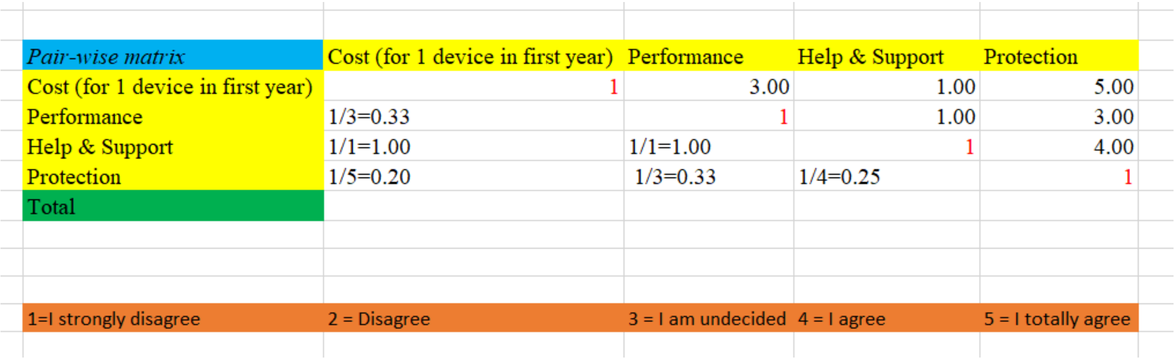
Depending on the results above, we see that there are some differences between the tests performed on antivirus programs and the results we may encounter in real life. According to these results, we understand that all antivirus programs provide reasonable protection for users. But antivirus programs have developed so much today that we are trying to find out which is the best. Nevertheless, the development and improvement of antivirus programs provide users with a wide range of options to choose from and protect their devices from various threats.

4.10 Scoring Part

4.10.1 Analytic hierarchy process (AHP) Saaty’s Method

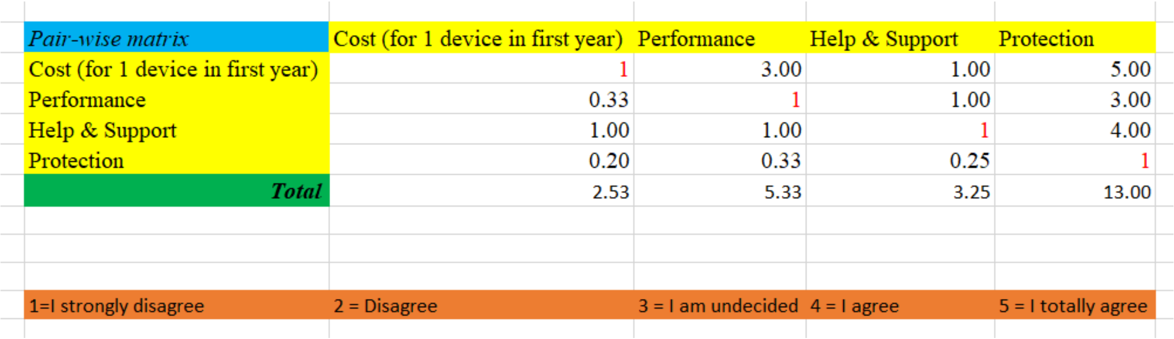
In this scoring section, we will apply the decision-making theory found by Thomas L. Saaty’s. The analytical hierarchy process (AHP) is an important tool in decision-making theory. AHP, it was developed by Thomas L. Saaty and provides a systematic approach to complex decisions, allowing for a better understanding and evaluation of alternatives. The main idea behind AHP is that it provides to break down a complex problem into simpler components so that each component can be evaluated separately before being combined into an overall solution or proposal. This allows better comparisons between different options and can help determine which option best suits the needs of an individual or organization. AHP uses mathematical models to analyze data from multiple perspectives, allowing users to make informed decisions more accurately than traditional methods.

In this method, we first defined 4 criteria. These criteria are Cost, Performance, Help & Support and Protection. In this method, this table is designed by giving numbers from 1 to 5. We have shown how these 4 different criteria are performed in weighting functions in antivirus programs. The first thing we did was to create a Pair-Wise matrix, that is, a comparative advantage matrix. This matrix shows us the comparison of the criteria among themselves. For this, we created a table in Excel and wrote the criteria one by one. Then, as we can see in the Table 4 below, the diagonals in the table are shown as 1. This is a rule of the Saaty‘s Method. This comparative advantage is the superiority of each criterion to itself 1. Then we ask questions about how important each criterion is between them and we make a Scoring. After determining the corresponding values, we first divided the underlying values (1/) and obtained the underlying values. Then, after writing down the total numbers, we obtained the Normalized Matrix A.



Pair-wise matrix	Cost (for 1 device in first year)	Performance	Help & Support	Protection
Cost (for 1 device in first year)	1	3.00	1.00	5.00
Performance	1/3=0.33	1	1.00	3.00
Help & Support	1/1=1.00	1/1=1.00	1	4.00
Protection	1/5=0.20	1/3=0.33	1/4=0.25	1
Total				
1=I strongly disagree	2 = Disagree	3 = I am undecided	4 = I agree	5 = I totally agree

Table 4:Saaty’s Method Table From Excel



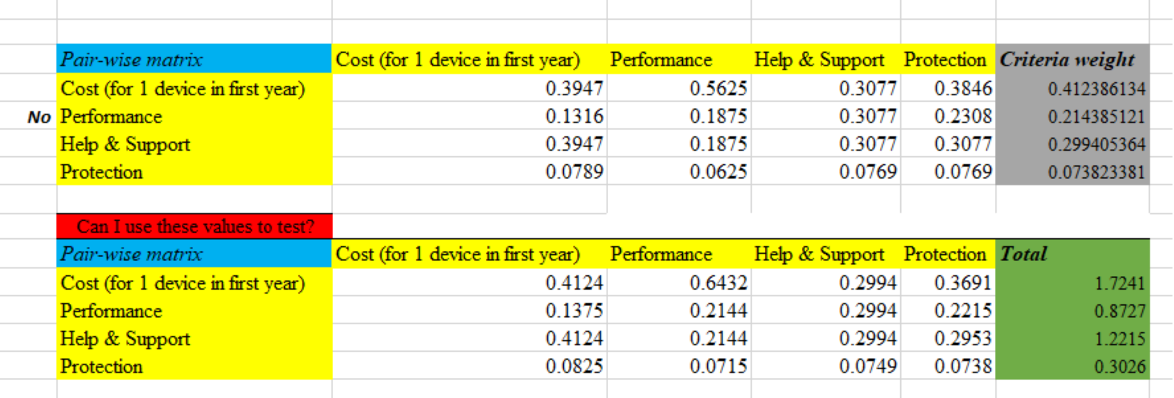
Pair-wise matrix	Cost (for 1 device in first year)	Performance	Help & Support	Protection
Cost (for 1 device in first year)	1	3.00	1.00	5.00
Performance	0.33	1	1.00	3.00
Help & Support	1.00	1.00	1	4.00
Protection	0.20	0.33	0.25	1
Total	2.53	5.33	3.25	13.00
1=I strongly disagree	2 = Disagree	3 = I am undecided	4 = I agree	5 = I totally agree

Table 5:Analytic hierarchy process (AHP) Saaty’s Method Table 2

4.10.2 Normalized A Matrix Table

In this table 6, we divide the first value and the Total number in the Cost section, and after obtaining the number, we find the other values by performing the same operations in the others one by one. After finding the values of all of them, we proceed to find the Criterion Weights. To get the criterion weights, as we can see in the table below (Pair-wise Method), we add the Cost section under and get the Criterion weights. By performing this operation within the other Criteria, we find the Criterion Weights of all of them. After finding the Criteria Weights, can we use the criteria figures we found (In my analysis?) so will it give results that will give hope for the future? We are also testing it in the other table below.

In the table below, we look at the first table we made and take the figure from the first observation. We multiply the number we get by the Criterion Weight result in the second table. We multiply the results we find in the Criterion Weight one by one with the numbers in the first table and find the results of all of them. Then we collect the numbers we found. After performing the addition operations, we need to divide the Total values and the Criterion Weights by each other and take the average to find the Lambda value. The average result we found gives us our Lambda result. After finding the result in Lamda, we apply the formula to find the Consistency Index (CI) result.

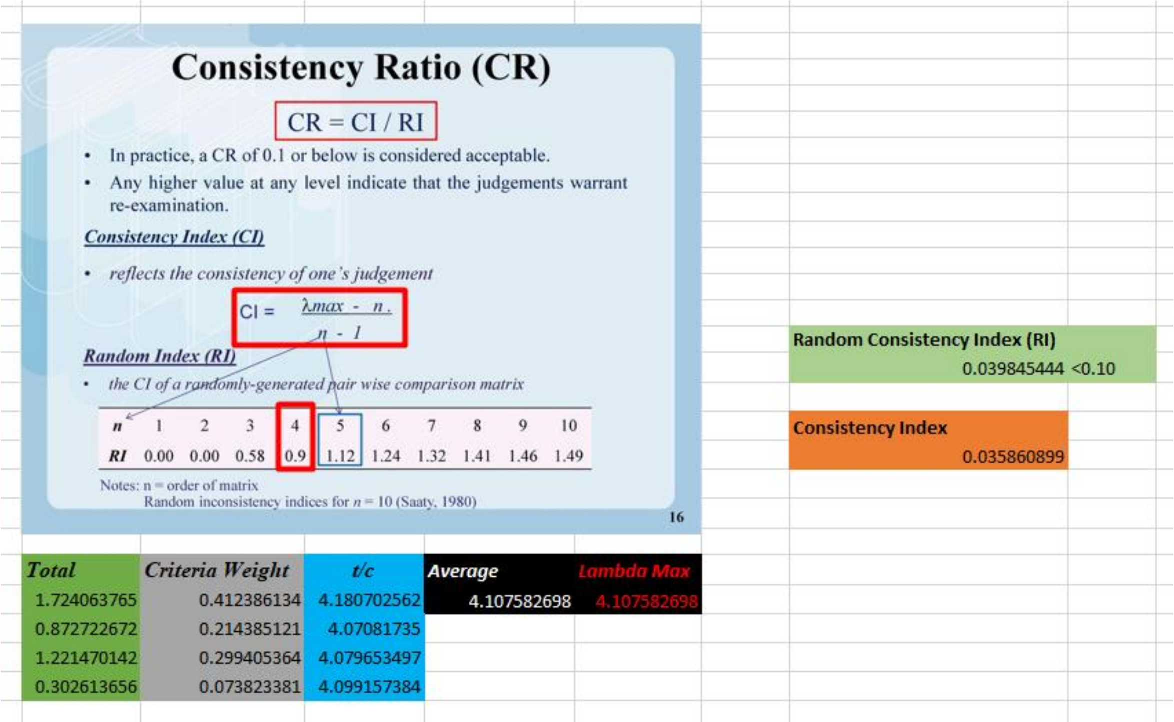


	Pair-wise matrix	Cost (for 1 device in first year)	Performance	Help & Support	Protection	***Criteria weight***
	Cost (for 1 device in first year)	0.3947	0.5625	0.3077	0.3846	0.412386134
No	Performance	0.1316	0.1875	0.3077	0.2308	0.214385121
	Help & Support	0.3947	0.1875	0.3077	0.3077	0.299405364
	Protection	0.0789	0.0625	0.0769	0.0769	0.073823381
	Can I use these values to test?					
	Pair-wise matrix	Cost (for 1 device in first year)	Performance	Help & Support	Protection	***Total***
	Cost (for 1 device in first year)	0.4124	0.6432	0.2994	0.3691	1.7241
	Performance	0.1375	0.2144	0.2994	0.2215	0.8727
	Help & Support	0.4124	0.2144	0.2994	0.2953	1.2215
	Protection	0.0825	0.0715	0.0749	0.0738	0.3026

Table 6:Analytic hierarchy process (AHP) Normalized A Matrix Table

4.10.3 Consistency Index and Random Consistency Index

In the Table 7 below, we write the Lamda Max value using the Consistency Index (CI) formula (Lamda Max – n / n – 1), and our number n is n=4 since we have 4 criteria. Therefore, by replacing them in the formula, we obtain our Consistency Index (CI) number ((Lamda Max – 4) / 3). The Consistency Index (CI) number is (0.03586089). After finding the number of the Consistency Index (CI), we can find the number of the Random Consistency Index (RI) using the number 0.9 in the table, as you can see in the table below, to find the number of Random Consistency Index (RI), because the number n indicates our criterion values, n is 4 in our result. To see this number, we find the Random Consistency Index (CI) number by dividing the Consistency Index (CI) number by 0.9. The Random Consistency Index number is (0.0398454).



Consistency Ratio (CR)

CR = CI / RI

- In practice, a CR of 0.1 or below is considered acceptable.
- Any higher value at any level indicate that the judgements warrant re-examination.

Consistency Index (CI)

- *reflects the consistency of one's judgement*

$$CI = \frac{\lambda max - n.}{n - 1}$$

Random Index (RI)

- *the CI of a randomly-generated pair wise comparison matrix*

n	1	2	3	4	5	6	7	8	9	10
RI	0.00	0.00	0.58	0.9	1.12	1.24	1.32	1.41	1.46	1.49

Notes: n = order of matrix
Random inconsistency indices for *n* = 10 (Saaty, 1980)

16

Total	*Criteria Weight*	*t/c*	*Average*	*Lambda Max*
1.724063765	0.412386134	4.180702562	4.107582698	4.107582698
0.872722672	0.214385121	4.07081735		
1.221470142	0.299405364	4.079653497		
0.302613656	0.073823381	4.099157384		

Random Consistency Index (RI)	
0.039845444	<0.10

Consistency Index
0.035860899

Table 7:Analytic hierarchy process (AHP) Consistency Index and Random Consitency Index Results

5 Conclusion

In conclusion, this thesis presents a comprehensive evaluation of the effectiveness of four popular antivirus software programs in the realm of cybersecurity. The performance test and Saaty’s method evaluation demonstrate that Kaspersky and Bitdefender are the most effective in protecting against cyber threats. Nonetheless, all four programs display strong capabilities in virus detection and removal. Therefore, it is highly recommended that individuals and organizations invest in reputable antivirus software to enhance their cybersecurity measures and minimize the risk of cyber attacks. In light of these limitations, future research could delve further into the impact of other factors, including network configuration and system requirements, on antivirus software performance.

The findings of this study highlight the importance of antivirus software in combating cyber threats. The study underscores the significance of reliable antivirus software in preventing malware infections and minimizing the risk of data breaches. By investing in reputable antivirus software, individuals and organizations can bolster their cybersecurity measures and safeguard their systems from cyber-attacks.

6 References

[1] I. Priyadarshini, Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies, R. K. B. K. M. M. K. J. M. C. DacNhuong Le, Ed., Wiley Online Library, 2019, p. 37.

[2] Z. H. L. &. A. H. L. Gurdip Kaur, Understanding Cybersecurity Management in FinTech, Springer Link, 2021, pp. 17-34.

[3] J. D. I. Chwan-Hwa (John) Wu, Introduction to Computer Networks and Cybersecurity, Boca Raton: Taylor & Francis Group, 2013, p. 1336.

[4] C. V. J. N. Jyri Rajamäki, Artist, *Cybersecurity versus information security.* [Art]. ResearchGate, 2018.

[5] B. D. Thierry Mbah Mbelli, “IEEE Xplore,” 18 August 2016. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7545887.

[6] P. J. D. Dorothy E. Denning, “ACM Digital Library,” 01 September 1979. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/356778.356782.

[7] G. Marin, “IEEE Xplore,” 12 December 2005. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1556540/authors#authors.

[8] M. M. P. F. William Hurst, Critical Infrastructure Protection VIII, S. S. Jonathan Butts, Ed., Springer Link, 2014, pp. 127-138.

[9] K. C. Ashish Singh, Journal of Network and Computer Applications, ScienceDirect, 2017, pp. 88-115.

[10] Y. S. C. P. JaeKwan Park, Progress in Nuclear Energy, ScienceDirect, 2016, pp. 88-94.

[11] C. C. ,. O.-G. ,. O. A. Aarón Echeverría, “MDPI,” 06 April 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/7/3260.

[12] K. T. B. A. Md Liakat Ali, “ACM Digital Library,” 02 July 2019. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3327960.3332393?casa_token=Zj6xQ55Q5WYAAAAA:Mtf30UiqOy82JffVSmZ7ipvqhPkp4uG8dMFVk_yTdcUqhRPb54wfvpzR6xPc8o3VZlAISH-MIhP0.

[13] Q. L. Yuchong Li, Energy Reports, ScienceDirect, 2021, pp. 8176-8186.

[14] B. Watkins, August 2014. [Çevrimiçi]. Available: http://www.amo.cz/wp-content/uploads/2015/11/amocz-BP-2014-3.pdf.

[15] M. S. ,. R.-G. ,. S. ,. L. D. ,. T. Iheanyi Nwankwo, “MDPI,” 21 March 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/6/965.

[16] M. L. A. ,. T. Beatrice Atobatele, “ACM Digital Library,” 02 July 2019. [Online].

[17] B. H. N. A. K. S. Hadi Habibzadeh, Sustainable Cities and Society, ScienceDirect, 2019.

[18] T. K. H. K. R. K. Diptiben Ghelani, “Authorea,” 22 September 2022. [Online]. Available: https://www.authorea.com/doi/full/10.22541/au.166385206.63311335.

[19] I. H. Sarker, “Springer Link,” 20 March 2021. [Online]. Available: https://link.springer.com/article/10.1007/s42979-021-00535-6.

[20] C. S. ,. B. J. T. M. D. K. Kruse, “IOS Press,” 21 February 2017. [Online]. Available: https://content.iospress.com/articles/technology-and-health-care/thc1263.

[21] M. Q. K. G. M. L. A. Kutub Thakur, “IEEE Xplore,” 07 January 2016. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7371499/authors#authors.

[22] M. K. ,. B. Parneet Kaur, “Taylor and Francis Online,” 20 July 2017. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/21642583.2017.1331768.

[23] J. R. W. W. L. S. W. Z. Q. Y. Senming Yan, “IEEE Xplore,” 28 November 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9964330/authors.

[24] S. A. C. ,. G. R. Junaid Ahsenali Chaudhry, 2016. [Online]. Available: https://d1wqtxts1xzle7.cloudfront.net/67348149/ijsia.2016.10.1-libre.pdf?1621266006=&response-content-disposition=inline%3B+filename%3DPhishing_Attacks_and_Defenses.pdf&Expires=1677594350&Signature=DM9G1UUzvn9DY9MCnI6V6lVNU~NdYEW3AFImrOoga89hF43JP81xpFFIE.

[25] R. S. B. N. K. Akarshita Shankar, “Ripublication,” 2019. [Online]. Available: https://www.ripublication.com/ijaer19/ijaerv14n9_15.pdf.

[26] A. A. ,. A. S. U. ,. K. ,. A. S. Ege Tekiner, “IEEE Xplore,” 04 November 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9581251/authors#authors.

[27] J. H. ,. G. ,. M. B. Christian W. Probst, Insider Threats in Cyber Security, J. H. D. G. M. B. Christian W. Probst, Ed., Springer New York, NY, 2010, pp. 5-244.

[28] D. watson, Artist, *Introduction to Cyber Security.* [Art]. The Engineering Projects, 2020.

[29] M. F. Z. Chai Kar Yee, Review on Confidentiality, Integrity and Availability in Information Security, Universiti Pendidikan Sultan Idris, 2021.

[30] N. M. Jasber Kaur, “ IEEE Xplore,” 23 January 2014. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6716723/authors#authors.

[31] S. S. David Coss, “Journal of Information System Security,” 2014 . [Online]. Available: https://www.proso.com/dl/Samonas.pdf.

[32] T. L. Saaty, The Analytic Hierarchy and Analytic Network Processes for the Measurement of Intangible Criteria and for Decision-Making, Springer, New York, NY, 2016, p. 57.

[33] R. A.-A. A. M. Abdel Rahman Al-Shabeeb, “Scientific Research,” 27 October 2016. [Online]. Available: https://www.scirp.org/(S(lz5mqp453edsnp55rrgjct55))/reference/ReferencesPapers.aspx?ReferenceID=1895817.

[34] R. P. Antonio Pérez-Sánchez, “MDPI,” 20 January 2022. [Online]. Available: https://www.mdpi.com/2076-3417/12/3/1076.

[35] A. V. Catalin BOJA, “Electronic Identity Using Multi-Application Smartcards,” 2007. [Online]. Available: https://www.revistaie.ase.ro/content/44/20%20boja.pdf.

[36] U. H. R. &. U. Nayak, “Springer Link,” 01 January 2014. [Online]. Available: https://link.springer.com/chapter/10.1007/978-1-4302-6383-8_7.

[37] K. Glamoslija, “ESET Antivirus Review 2023: Is It Any Good?,” 27 February 2023. [Online]. Available: https://www.safetydetectives.com/best-antivirus/eset/.

[38] G. Held, “Wiley Online Library,” 06 September 2006. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/nem.623.

[39] N. Kshetri, “Emerald insight,” 01 July 2011. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/20450621111180954/full/html.

[40] W. R. Stewart Wolpin, “McAfee Antivirus Review and Prices,” 16 May 2022. [Online]. Available: https://www.usnews.com/360-reviews/privacy/antivirus/mcafee.

[41] I. Paul, “McAfee Total Protection review: Top security, but the app needs a little work,” 01 March 2022. [Online]. Available: https://www.pcworld.com/article/407405/mcafee-total-protection-review.html.

[42] M. Williams, “Bitdefender Antivirus review,” 10 December 2021. [Online]. Available: https://www.techradar.com/reviews/bitdefender-antivirus.

[43] AV-Comparatives, “AV Comparatives,” 08 October 2022. [Online]. Available: https://www.av-comparatives.org/tests/performance-test-october-2022/.

Appendix

Interview Part

After negotiations with antivirus companies, only ESET antivirus provided a return. Other antivirus companies have informed that they cannot return to the interview due to company policies, and the answer has been given according to the procedures.

Questions about ESET Antivirus program
Interviewed = Ondrej Safar
Position: Senior PR & Communications Manager at ESET Česká republika

1- **It is known in the world that ESET antivirus program provides a lot of protection for personal use (Home use). Do you think the ESET antivirus program is very good condition for home use? If the in company use, is it low in protection against other competitors? Or Is the antivirus program good against other competitors in company use?**

- For decades ESET home users as well as for all types of companies is one of the best software to protect against cyber threats and cyber attack every 39 seconds more than 2000 per day so we can say that a cyber attack has occurred. ESET's protection rate is 99.9%.

2- As far as I know, too many people in the world use ESET antivirus system. What is your current number of users and how many cyber attacks do you protect per day?

- Today, more than 110 million users worldwide use ESET software for protection but more than 1 billion users are protected but ESET technology because it is built into Google Chrome. And every single day we detect more than 400 thousand samples of new malware. So the number of prevented cyber attacks is very, very large.

3- **What criteria does ESET antivirus use to detect threats?**

- In addition to products that work in different security layers, ESET's 16 different modules work in an integrated way so that it can make these detections only in the product that works on the endpoint. According to the type of attack; For example, if it is a network attack, the “Network Protection” modules, if it is ransomware, the “Ransomware Protection” modules can block threats.

The work of new generation threats with heuristic methods such as "Advanced Machine Learning" and "Advanced Memory Scanner" along with classical detection methods increases protection.

4- **What are the most important variables in ESET antivirus program Malware protection? What is the rate of protection of incoming attacks in your opinion?**

- The most important variables in ESET antivirus malware protection are detection rate, scanning speed and system resources. The detection rate refers to how effectively the software can detect malicious programs; scanning speed is how fast it can identify threats; and system resources refer to how much of your computer's memory, processing power, and storage space will be used by the program. All three of these variables should be taken into account when choosing an antivirus solution for optimum protection against malware threats. ESET's protection rate is 99.9%.

5- **Which antivirus is your main competitor and what are the advantages of ESET antivirus over your competitors?**

- It would not be correct to say our main competitor. But I can talk about our advantages over other Antivirus programs. While ESET Antivirus offers excellent protection, it has many advantages that set ESET apart from its competitors.

One of the key advantages that sets ESET apart from other solutions is its multi-layered approach to security. This includes both signature-based detection and behavior tracking technology that allows it to detect malicious activities even if signatures have not yet been created for them. It also uses proactive heuristics that can detect suspicious behavior before an attack occurs, allowing users to take preventative measures before any damage occurs.

Finally, what I can say in this question is that it has a user-friendly interface that makes it easy to install and configure even for novice users. While it offers advanced options such as customizing scan settings or creating exclusion lists, unwanted software will not be scanned during routine checks and it will save valuable system resources while keeping your computer safe by scanning unnecessary items and ensuring that only essential items are checked without wasting time. This makes it a strong choice among the Antiviruses currently available.

6- In my thesis, I researched 4 antivirus programs and performed performance tests. In this performance test, I noticed that ESET antivirus uses much less CPU and Memory than other antivirus programs. It seems that you have worked very hard not to degrade the performance of the users' computers using your antivirus program and you have achieved great success. But after starting the virus scan, It performed poorly in finding viruses compared to other antivirus programs and found fewer viruses than other programs. Could you tell us about the work you will do to improve all these deficiencies and to become a leader?

- It is correct that ESET products use less CPU and memory than other products. ESET engine works very efficiently. On the other hand, I can not explain the results of your test without knowing the methodology that had been used. But in general, one of the biggest advantages of ESET is the smaller number of so-called false positives than other products. To show fewer threats than other products does not have to be a necessarily bad thing.