MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
VASYL' STUS DONETSK NATIONAL UNIVERSITY

HARRISON ASAMOAH

Admitted to defense:
Head of Information Technologies Department,
Ph.D., Associate Professor
_____ Tetyana V. Neskorodieva
«____» _____ 2021

ANTIVIRUS SOFTWARE VERSUS MALWARE

122 Computer science

Qualifying (Bachelor's) thesis

Supervisor:
Maryna O. Iepik,
Associate Professor of Information Technologies Department,
Ph.D., Associate Professor of Computer Technology

Point: ____ / ___ / _____
(points/scale ECTS/national scale)
Head of EC: _____
(signature)

Vinnytsia 2021

ABSTRACT

People use computers for all kind of activities: online gaming, shopping, entertainment, emails, Facebook, study, research, etc. At the same time, the risk of infection by malicious programs in these computers is rising. The main issue is that general users don't understand what a malware is and how computers get infected. On the other hand, many vendors produce antivirus software with different features to prevent or remove this malware from people's computers. General users don't understand the concept of each feature in these programs, nor is there a tool to advise users about what the features mean and help them select the right software for personal or business needs. The purpose of this paper is to make known the uses of antivirus, the types, how to prevent your computers from getting infected and also to know the dangers involve in malwares, the types and how you can get infected.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Antivirus software is a class of program designed to prevent, detect and remove malware infections on individual computing devices, networks and IT systems. Antivirus software is special security software that aims to give better protection than that offered by the underlying operating system (such as Windows or Mac OS X). In most cases, it is used as a preventive solution.

However, when that fails, the Antivirus (AV) software is used to disinfect the infected programs or to completely clean malicious software from the operating system. AV software uses various techniques to identify malicious software, which often self-protects and hides deep in an operating system.

Advanced malware may use undocumented operating system functionality and obscure techniques in order to persist and avoid being detected. Because of the large attack surface these days, AV software is designed to deal with all kinds of malicious payloads coming from both trusted and untrusted sources.

Some malicious inputs that AV software tries to protect an operating system from, with varying degrees of success, are network packets, email attachments, and exploits for browsers and document readers, as well as executable programs running on the operating system.

Antivirus or anti-virus software (often abbreviated as AV), sometimes known as anti-malware software, is computer software used to prevent, detect and remove

malicious software. Antivirus software was originally developed to detect and remove computer viruses, hence the name. However, with the proliferation of other kinds of malware, antivirus software started to provide protection from other computer threats. In particular, modern antivirus software can protect from: malicious Browser Helper Objects (BHOs), browser hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraud tools, adware and spyware [1].

Some products also include protection from other computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, Advanced Persistent Threat (APT), botnets, DDoS attacks [2].

Although the roots of the computer virus date back as early as 1949, when the Hungarian scientist John von Neumann published the “Theory of self-reproducing automata” [3], the first known computer virus appeared in 1971 and was dubbed the “Creeper virus” [4]. This computer virus infected Digital Equipment Corporation's (DEC) PDP-10 mainframe computers running the TENEX operating system [5,6].

The Creeper virus was eventually deleted by a program created by Ray Tomlinson and known as “The Reaper” [7]. Some people consider “The Reaper” the first antivirus software ever written – it may be the case, but it is important to note that the Reaper was actually a virus itself specifically designed to remove the Creeper virus [7,8,9]. The Creeper virus was followed by several other viruses. The first known that appeared “in the wild” was "Elk Cloner", in 1981, which infected Apple II computers [10,11,12].

In 1983, the term “computer virus” was coined by Fred Cohen in one of the first ever published academic papers on computer viruses [13]. Cohen used the term “computer virus” to describe a program that: “affect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself” [14] (note that a more recent, and precise, definition of computer virus has been given by the Hungarian security researcher Péter Szőr: “a code that recursively replicates a possibly evolved copy of itself” [15,16]).

The first IBM PC-compatible “in the wild” computer virus, and one of the first real widespread infections, was "Brain" in 1986. From then, the number of viruses has grown exponentially [17,18]. Most of the computer viruses written in the early and mid-1980s were limited to self-reproduction and had no specific damage routine built into the code.

That changed when more and more programmers became acquainted with computer virus programming and created viruses that manipulated or even destroyed data on infected computers.

Before internet connectivity was widespread, computer viruses were typically spread by infected floppy disks.

Antivirus software came into use, but was updated relatively infrequently. During this time, virus checkers essentially had to check executable files and the boot sectors of floppy disks and hard disks. However, as internet usage became common, viruses began to spread online [19].

From first computer virus Creeper created in the 1970s which is spread across the network with a message displaying “I’m the creeper, catch me if you can!”, until

today's advanced threats, security experts from around the globe are trying to fight against these malicious threat actors.

But as in a real physical world, criminals are always one step ahead and this battle is a continuous process which will never end. But as a user we can do much to apply security measures recommended from these security experts to minimize the attack vector and maximize the protection of our assets.

Malware, short for malicious (or malevolent) software, is software used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

It can appear in the form of code, scripts, active content, and other software. "Malware" is a general term used to refer to a variety of forms of hostile or intrusive software. Malware includes computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs and other malicious programs; the majority of active malware threats are usually worms or trojans rather than viruses [1].

There was some malware for other platforms before 1986., but in 1986 appeared first malware for PC. It was virus called Brain.A. Brain.A was developed in Pakistan, by two brothers – Basit and Amjad.

They wanted to prove that PC is not secure platform, so they created virus that was replicating using floppy disks. It infected booting sector of floppy drive and booting sector of every inserted floppy disk.

So anytime infected floppy would be inserted into PC, it would infect it's drive, so the drive would infected again every disk inserted of network worms. These threats become popular when internet becomes wide spread.

1.1 Types of Antivirus Software

Anyone who finds out on the internet and then knows about various antivirus programs can benefit by allowing you to stay safe when you are online. Accessing a website can open the way for hackers to infect your computer with a virus, and they are also able to gather information or spying on you secretly [20].

Not only antiviruses that have various types, but computer malwares also have various types. You should also learn the types of computer malwares to know how to counteract and fix them. But you don't need to worry, by installing appropriate antivirus software, you can prevent viruses from infiltrate your computer or smartphone

Some examples of types of antivirus software are McAfee, Kaspersky, AVG, Norton and many more.

This article was Posted by numbones.com with title
“Antivirus: Definition,Types, and Examples - numbones.com”
For more information, visit https://www.numbones.com/2019/01/antivirus.html

1.2 Types of Malware

When people are surfing the internet, they tend not to worry about the topic of internet security, and they accidentally download a malware when they least expect it. However, it is important to understand different types of malware and what they are capable of performing (Roger, 2018).

"Malware" is an abbreviation of the term "malicious software". That refers to code which has been created deliberately harmful. The malware can manipulate, delete, move and/or copy data or disrupt the workflow of the computer or network. In addition, malware also can aim damaging of the physical hardware of the systems (Cisco, 2018). Some examples are viruses, worms, Trojans, Ransomware, Logic Bombs and many more.

Each of these malware types has its own peculiarities and malice and is fundamentally different from another.

Often it is difficult to clearly assign a given malware to a class. For example, some malwares belong to both the virus and the worm category because it contains properties of both (Cisco, 2018).

Antivirus	Malware
AVG, McAfee, Norton	Virus, Keyloggers, Worms
Kaspersky, Ad Aware, ESET	Trojans, Ransomware, Logic Bombs
Avast, Panda, Avira, Bitdefender, etc	Bots/Botnets, Adware and Spyware, etc

CHAPTER 2

LETERATURE REVIEW

Malware is a general term that encompasses viruses, Trojans, spywares and other invasive code is widespread today. Malware analysis is a multistep process providing insight into malware structure and functionality, facilitating the expansion of remedy. According to researcher:

1) (Christodorescu et al., 2005) described a malware instance as a program whose objective is malevolent [20].

2) (McGraw and Morrisett,2000) defined malicious code as “any code added, changed, or removed from a software system in order to intentionally cause harm or subvert the intended function of the system” [21].

3) The description given by (Vasudevan and Yerraballi, 2006) which described malware as “a generic term that encompasses viruses, trojans, spywares and other intrusive code” [22].

4) (Aycock, 2006) defined malware as “software whose intent is malicious, or whose effect is malicious” [23].

5) The term “malware” here is being used as the generic name for the class of code that is malicious, including viruses, trojans, worms, and spyware. Malware authors use generators, incorporate libraries, and borrow code from others—there exists a robust network for exchange, and some malware authors take time to read and understand prior approaches by (Arief & Besnard, 2003) [24].

6) (Fred Cohen's) original definition of a computer virus as of 1983 was: “a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself”. He updated this definition a year later in 1984 in his paper entitled: “Computer Viruses – Theories and Experiments”.

7) According to BBC News online, 2004 malware is a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners.

8) (Skoudis and Zeltser, 2003) [25]. Malware is a set of instructions that run on your computer and make your system do something that an attacker wants it to do.

The term computer virus was first used in a science fiction novel by (Gerrold, 1972), which includes a description of a fictional computer program called virus and was able to self-replicate. The first academic use of the term was claimed by (Cohen, 1983).

The first published account of the term can be found a year later by (Cohen, 1984) in his paper Experiments with Computer Viruses. Though Cohen first used the term, some early accounts of viruses can be found. According to (Ferbrache, 1992), the first reported incidents of true viruses were in 1981 and 1982 on the Apple II computer.

Elk Cloner is considered to be the first documented example of a virus in mid-1981. The first PC virus was a boot sector virus called Brain in 1986, (Hoffman, 1990). Worm also owes their existence to science fiction literature.

(Brunner’s, 1975) Shockwave Rider introduced us to worm, a program that propagates itself on a computer network. (Shoch, 1982) claimed the first use of the term in academic circles. Much has been written about viruses, worms, trojans and other

malwares since then, but now we shift our focus, from fiction to the real world where both malware and anti-malware are big commercial industries now (Gutmann, 2007).

2.1 Malware Analysis

Malware analysis is a multi-step process providing insight into malware structure and functionality. Behavior monitoring, an important step in the analysis process, is used to observe malware relations with respect to the system and is achieved by employing dynamic coarse-grained binary-instrumentation on the target system. Initial examination of collected malware is called profiling (Aquilina et al., 2008).

Dataflow analysis examines the way data is moved and changed throughout the execution of a program (Chess et al., 2007). (Skoudis, 2004) outlined a model where analysis tools are distributed on a local victim machine and on an external machine, to capture behavioral aspects of the malware on the local machine and its interaction with external services over a network. External services as outlined by (Arnold et al., 2000) can be setup on the external monitoring segment.

(Rieck et al.) experimented with different heterogeneous test data collected over several months using honeypots demonstrated the effectiveness of the method, especially in detecting novel instances of malware families previously not recognized by commercial antivirus software.

A number of analysis tools are utilized by malware forensic analysts, with static and dynamic analysis representing two significant methodologies that can be used to analyse malware (Aquilina et al., 2008).

Software disassemblers and debuggers such as IDA Pro (Hex-Rays, 2008) and OllyDBg (Yuschusk, 2008) can be used to perform a detailed analysis of the malware code and provide an internal view of the malwares functionality (Valli & Brand, 2008). This is referred to as static analysis. In contrast, dynamic analysis runs the malware and observes the interaction of the running malware with the computer from a behavioural point of view. A number of plug-ins that extend the functionality of IDA Pro and OllyDBg include IDA Stealth (Newger, 2008) and Olly Advanced (MaRKuS, 2006) respectively to work with malicious code that employ anti-analysis techniques.

The intention of such plug-ins is to provide functionality to hide their associated tools. Extensive literature exists on static analysis of malicious binaries, e.g. (Christodorescu et al., 2005; Kirda et.al, 2006; Kruegel et.al, 2004) [25].

Moreover, recent work of (Moser et al., 2007) presents obfuscation techniques that are provably NP-hard for static analysis. Dynamic malware analysis techniques have previously focused on obtaining reliable and accurate information on execution of malicious programs (Bayer et al., 2006; Moser et al., 2007; Willems et al., 2007).
Two techniques for behavior-based malware analysis using clustering of behavior reports have been recently proposed (Lee et al., 2006; Bailey et al., 2007).

(Moser et al., 2007) proposed a system that dynamically monitors a suspicious program to identify the execution points where the application makes control flow decisions based on input-dependent values.

Static Anomaly Detection (Wagner, 2011)

Proposed a technique that created a control flow graph (CFG) for a program representing its system call trace. At execution time this CFG was compared with the system call sequences to check for any violation.

Hybrid Anomaly Detection (Rabek, 2003)

Proposed an anomaly based technique where static analysis was assisted by dynamic analysis to detect injected, dynamically generated and obfuscated code. Within the program static analysis was used to identify the location of system calls.

The programs can be dynamically monitored later to verify that each realistic system call is made from the same location well-known using the static analysis.

Static Misuse Detection (Bergeron et al., 1999)

Used a static misuse detection scheme where they used program slicing to extract program regions that are critical from a security point of view. In a related work (Bergeron et al., 2001) extracted an API call graph instead of the program slices to test against the security policy. (Lo et al., 1995) proposed the idea of tell-tale signs which were heuristic signatures of malicious program.

Dynamic Anomaly Detection (Hofmeyr et al., 1998)

Proposed anomaly detection based upon sequence of system calls. A normal profile was composed of short sequence of system calls. In a similar approach (Sekar

et al. 2001) used Finite State Automata (FSA) to represent system call sequences. Similarly, (Ko et al., 1997) proposed an idea of trace policy which was essentially a sequence of system calls in time (Masri et al., 2005) presented a tool called Dynamic Information Flow Analysis (DIFA) to monitor method calls at runtime for Java applications (Sekar et al., 1999) created a system call detection engine that compares system calls modeled previously with the system calls made at runtime.

Hybrid Misuse Detection (Mori, 2004)

Presented an approach to detect encrypted and polymorphic viruses using static analysis and code emulation.

Dynamic Misuse Detection (Debbabi, 2001)

Proposed a dynamic monitoring system that enforces a security policy. The approach was implemented in a system called DaMon. Schneider 1998 presented enforceable security policies in the form of Finite State Automata. (Vasudevan et al.) have developed a new dynamic coarse-grained binary instrumentation framework codenamed SPiKE, that aids in the construction of powerful malware analysis tools to combat malware that are becoming increasingly hard to analyze.

Goal is to present a binary instrumentation framework that is unremarkable, moveable, capable, easy-to-use and reusable, supporting multithreading and SM-SC code, both in user- and kernel-mode.

(Valli et al.) laid an establishment for a Malware Analysis Body of Knowledge (MABOK) which is required to analyze the malware forensically. This body of

knowledge has been the outcome of several years of study into malware categorization. Debuggers such as OllyDbg (Yuschuk, 2008) and IDA Pro (Hex Rays, 2008) are commonly used for the analysis of malware.

Plugins such as Olly Advanced (MaRKuS, 2006) for OllyDbg and IDA Stealth (Newger, 2008) for IDA Pro focus on hiding the presence of the tool from the software under investigation, in an effort to avoid detection. (Christodorescu et al.) presented a unique viewpoint on malicious code detection.

Attacker who writes the malicious code tries to conceal the malicious code to threaten the malicious code detectors such as Anti- virus software. (Bayer et al.) presented TT Analyze, a tool for dynamically analyzing the behavior of Windows executables. Binary is run in an emulated operating system environment and the actions are monitored.

It does not modify the program it executes which one of the most important aspects of the system is making it more difficult for the malicious code to be detected. This tool runs the binaries in unchanged Windows environment making it accurate.

Therefore, these factors make TT Analyze a perfect tool for quickly getting an accepting of the behavior of an unknown malware.

CHAPTER 3

METHODOLOGY

3.1 How antivirus software works

Antivirus software typically runs as a background process, scanning computers, servers or mobile devices to detect and restrict the spread of malware. Many antivirus software programs include real-time threat detection and protection to guard against potential vulnerabilities as they happen, as well as system scans that monitor device and system files looking for possible risks.

Antivirus software usually performs these basic functions:

1) Scanning directories or specific files for known malicious patterns indicating the presence of malicious software;
2) Allowing users to schedule scans so they run automatically;
3) Users to initiate new scans at any time;
4) Removing any malicious Software, it detects. Some antivirus software programs do this automatically in the background, while others notify users of infections and ask them if they want to clean the files.

In order to scan systems comprehensively, antivirus software must generally be given privileged access to the entire system. This makes antivirus software itself a

common target for attackers, and researchers have discovered remote code execution and other serious vulnerabilities in antivirus software products in recent years.

3.2 Virus detection techniques

Antivirus software uses a variety of virus detection techniques.

Originally, antivirus software depended on signature-based detection to flag malicious software. Antivirus programs depend on stored virus signatures -- unique strings of data that are characteristic of known malware.

The antivirus software uses these signatures to identify when it encounters viruses that have already been identified and analyzed by security experts.

Signature-based malware cannot detect new malware, including variants of existing malware. Signature-based detection can only detect new viruses when the definition file is updated with information about the new virus.

With the number of new malware signatures increasing at around 10 million per year as long ago as 2011, modern signature databases may contain hundreds of millions, or even billions, of entries, making antivirus software based solely on signatures impractical. However, signature-based detection does not usually produce false positive matches.

Heuristic-based detection uses an algorithm to compare the signatures of known viruses against potential threats. With heuristic-based detection, antivirus software can detect viruses that haven't been discovered yet, as well as already existing viruses that have been disguised or modified and released as new viruses.

However, this method can also generate false-positive matches when antivirus software detects a program behaving similarly to a malicious program and incorrectly identifies it as a virus.

Antivirus software may also use behavior-based detection to analyze an object's behavior or potential behavior for suspicious activities and infers malicious intent based on those observations.

For example, code that attempts to perform unauthorized or abnormal actions would indicate the object is malicious, or at least suspicious. Some examples of behaviors that potentially signal danger include modifying or deleting large numbers of files, monitoring keystrokes, changing settings of other programs and remotely connecting to computers.

3.3 The Benefits of Anti-Virus Software

When the end-user setup the anti-virus software on his personal computer, he gains the protection from viruses, spyware, Trojans, adware, worms, and others. Many users click on the attached files in emails or the suspect links, or they visit untrusted websites, so, by having the anti-virus program, the probability of getting infected can be decreased.

The virus is not only having the ability to do damage to the valued data, it also can make the PC useless by destroying the main functions and processes and the result of that is, the reduction of computer’s performance.

AV program will protect end user while he surfs the web, also it isolates and prevents hackers from accessing to personal things as: bank account access or credit card information.

The firewall property attached to many AV programs to block any unwanted (i.e. unauthorized) incoming connections, and to prevent hackers attacking end user system. When the viruses attack your personal computer, they can delete important personal images and files, slow down your processing speeds, and they lead to physical problem to your computer that cannot be fixed.

The AV program can protect your computer from the identity theft and spyware. Identity theft is a major problem for the victims, and it can cause many problems as receive bad marks on the user's credit report and lost money.

The spyware is a type of software that is designed to attack computer and spy on the users of it, the spyware looking for and get all personal information that stored on a personal computer, this can be: passwords, data about financial issues, the number of credit card and social security.

The hackers can use the information in a wrong way that can harm the victim.

The AV program protects your PC from Spam, which is annoying you. In most time, the spam is the result of a virus stored on your computer; you can recognize that situation when your PC gets many emails and ads, that you have no interest on it.

3.4 How malware works

Many early infectious programs, including the first Internet Worm, were written as experiments or pranks.

Today, malware is used primarily to steal sensitive personal, financial, or business information for the benefit of others.

Malware is sometimes used broadly against government or corporate websites to gather guarded information, or to disrupt their operation in general.

However, malware is often used against individuals to gain personal information such as social security numbers, bank or credit card numbers, and so on.

3.5 Types of Malware

Virus

Virus is the first category of malware to appear on the horizon of computer security. It is self-replicating in nature and is referred to as a parasitic infector. It does not have a separate existence; instead, it inserts its code into existing files on the system. It could be an executable program or script of different programming languages like VBScript, JavaScript, Perl, etc.

Worm

Worms are also self-replicating; however, they are standalone malware strains. They do not modify other files to spread; instead, they make copies of themselves over

network shares or on other systems. Worms are further classified based upon the spreading mechanism used such as email, P2P, IRC, etc.

Trojan

A Trojan is always disguised as useful software and tempts a user to install it and it is also bundled with hidden malicious functionality. It is non-replicating in nature, i.e. it does not spread in a similar manner as viruses or worms.

Backdoor

Backdoors allow unauthorized access to a compromised system by opening a port on the system. This creates a pathway for hackers to control the compromised system by sending commands of malicious nature.

SubSeven, NetBus and Back Orifice are some of the well-known examples of backdoors which enable unauthorized people to access user systems over the Internet without his/her knowledge.

HackTool

A HackTool is used by a hacker to attack and exploit a system to gain unauthorized access to system resources. It attempts to gain information about the system after bypassing security mechanisms that are inherent to the system. Netcat is an example of HackTool.

Sometimes it is even used by network administrators; however, it is mostly used by hackers to gain unauthorized access and to transmit data on a network.

Spyware

Spyware is software that gathers personal or confidential information from user systems without their knowledge. It includes monitoring the systems to collect information such as browsing habits, recently visited sites, passwords, credit card information, and other confidential information.

Once spyware is installed, it does not show any visible notifications to indicate that it is monitoring user activities. It instantly sends this information to the configured remote server.

Rootkit

Rootkits use stealth techniques to actively hide their presence by concealing their components such as files, registry keys, running processes and other objects.

These techniques are used to hide their behavior from users and to bypass detection from security applications.

Rogue application

These are fake applications which pose as security applications or system tools to mislead users into paying for the removal of non-existent malware or issues with their systems. This category of malware is on a steady rise over the last 4-5 years.

They use different social engineering techniques to mislead users into installing them. Their downloader components may come as video codecs to run certain video clips, P2P software or Trojanized shared applications.

Malware writers also use SEO poisoning techniques to push malicious URLs based on recent or popular news.

When a user visits such malicious URLs, rogue applications get downloaded using drive-by download techniques by exploiting vulnerabilities in web browsers and their plugins.

3.6 Infection Vectors

An infection vector refers to the spreading mechanism used by malware.

1) Boot Sector: Infecting Master boot record (MBR) of the physical disk;
2) File Infection: Parasitic infectors;
3) Email: Email worms;
4) File Shares: Parasitic infectors, worms;
5) Network: Network worms, through vulnerabilities;
6) IRC: Internet Relay Chat;
7) P2P Networks: IM, Kazaa, etc.;
8) Removable Media: Floppy, USB drives, optical discs;
9) Bluetooth: Worms for mobile devices;
10) Web Apps: Using cross-site scripting vulnerabilities;
11) Vulnerabilities: Operating system, Web browser and plugins, Adobe Reader vulnerabilities.

CHAPTER 4

DISCUSSION

The computer which we use today has become an important part in our daily lifes. Without them it is almost impossible for our daily works as well as our professions. And also when using them we always wanted to ensure safety and privacy especially from viruses.

Antivirus software is designed to remove viruses off your computer. Without an antivirus program your system will be vulnerable to viruses and other threats.

Apart from removing viruses, an antivirus software does have other major benefits. Whether it is a desktop used in home or office, it is essential for an antivirus software to be installed in them. While using them users can come across drawbacks as well.

In this chapter we'll talk more about the advantages and disadvantages of antivirus and malware.

4.1 Advantages of antivirus software

Virus Protection

The main role of an antivirus program is to stand against viruses and other forms of malwares. The viruses will not only cause damages to your data, it can degrade the overall system performance.

All of them can happen without your knowledge. The antivirus software installed on your computer detects and removes these malwares before they cause any harms to your computer.

Spyware Protection

Spyware as the name suggests is a kind of malware that spies on your computer stealing all the confidential information. These details also include credit card details, passwords and other financial data. This ultimately leads to identity theft.

The antivirus software has the capability to prevent these kinds of spyware attacks.

Web Protection

While surfing the internet, users can come across various other forms of threats. In an untrustworthy site, cyber attackers can gather your credit card and bank account details. One of the way to overcome this is by using an antivirus software.

Using antivirus program, you can protect your valuable information while surfing the web.

Spam Protection

Viruses can also enter your computer through means of spam emails and ads. These emails and ads can show up many times even if you have no interest in it.

Once the virus finds the way to sneak into your PC it causes irreversible damages. An Antivirus works by the way of blocking these spam emails and ads.

Firewall Feature

Most antivirus programs include a firewall feature in them. Antivirus program with firewall feature ensures 2-way protection to your PC. This means that whatever the information that is sent or received will be double checked here.

Therefore, no hackers can dig any personal information's from your system.

Cost Effective

Even though there are many premium versions of antivirus programs for a monthly/yearly subscription fee, there are some antivirus programs those are completely free of charge.

These kinds of antivirus programs offer almost the same level of protection provided by the subscription based. Even if you choose to afford a premium version, they are relatively inexpensive.

4.1.1 Disadvantages of Antivirus

System Slowdown

Using an antivirus program means that a lot of resources from the memory and the hard drive is being used. As a result, it can drastically slowdown overall speed of the computer. Moreover, the process of scanning can also cause lags in the network.

No Complete Protection

If you are using a free antivirus program, there is no guarantee that it will provide you the complete protection.

Most free antivirus programs out there only offer a basic level of protection.

Moreover, they are capable of identifying only certain types of threats. In order for acquiring complete level of protection, you have to use a firewall as well.

Security Holes

When security holes are present inside the operating system or the networking software, it will provide a chance for the virus to bypass the antivirus software.

Unless the user takes actions to keep it update, the antivirus software won't be effective.

Limited Detection Techniques

For identifying a potential threat, there are always more than one method available. However, in the case of antivirus program, it mostly executes the method of virus scanning.

Basically what happens in the process of scanning is, it will try to search for the virus code patterns. Sometimes the antivirus programs can give you false alarms if the scanning matches with the normal file.

Furthermore, if there are any new types of viruses the antivirus program will fail to identify it completely. That is the reason why antivirus software needs to be updated often.

Frequent Advertisements

Apart from premium versions of antivirus programs, through some means the free antivirus Software needs to generate an income.

Advertising is one of the ways to achieve them. Many at times these advertisements degrade user experience by showing up every time.

No Customer Support

Another drawback of a free antivirus program is that it lacks on the side of customer support. Unless you pay for the premium version, there won't be any customer support given to you.

In the event of any problem, the only way to overcome is through forums and knowledge bases.

4.2 Advantages of Malware

In short, malware can wreak havoc on a computer and its network. Hackers use it to steal passwords, delete files and render computers inoperable.

A malware infection can cause many problems that affect daily operation and the long-term security of your company.

Here are some of the many things malware can do.

Steal Your Sensitive Information

Information theft is one of the most serious and costly results of malware. Once pieces of malware such as spyware and trojans are installed on your device, hackers can gather your personal and company information to sell to third-party sources.

This information can include browsing history, passwords, client profiles and other sensitive data.

Slow Your Computer

Once a piece of malware is in action, it begins to consume a large chunk of your computer's memory. Many types of malware also replicate themselves and fill your hard drive, so there's little room left for legitimate programs.

This loss of space can lead to a sluggish computer, which makes it difficult to carry on with business as usual.

Restrict Access to Your Files

Certain types of malware can damage or delete files and programs on your computer. Unless your data is backed up on another hard drive or cloud server, you won't be able to regain access to many of these files.

Spread Throughout Your Network

Worms are an especially disruptive type of malware for businesses. Once this malware infects a computer, it replicates itself and spreads throughout the entire network.

Most companies operate all their devices on a single network — which means that a worm could damage not just one employee's computer, but the entire organization.

4.2.1 Symptoms of Malware

Because malware takes many different forms, it can look a bit different for everyone. However, some of the most common symptoms of a malware infection include next.

Slow computer

One of the most common signs of malware is a slow computer. As mentioned above, pieces of malware can noticeably slow down your operating system, programs and bandwidth.

Lack of storage

Malware can eat up storage space, leaving little room for legitimate programs and files.

If a plague of unfamiliar programs is slowing down your computer, search the programs' names online to make sure malware hasn't infected your device.

Crashing or freezing

Either technical problems or malware could cause regular computer crashes. Make sure that all your drivers are up to date and your programs are compatible with your hardware.

If it's not a hardware or software issue, malware might be causing your Blue Screen of Death.

Pop-ups and unwanted programs

Constant pop-ups or unfamiliar toolbars are one of the most annoying signs of malware. Don't click on any pages or toolbars that pop up out of the blue – close out of the program and run your anti-malware software immediately.

Spam

If your coworkers mention that they've been receiving messages from you that you don't remember sending, you're likely a victim of malware.

Caution them not to open any links or attachments within the messages.

4.3 How to prevent malware

When it comes to malware, prevention is better than a cure. Fortunately, there are some common sense, easy behaviors that minimize your chances of running into any nasty software.

Don't trust strangers online. Social engineering, which can include strange emails, abrupt alerts, fake profiles, and curiosity-tickling offers, is the most common method of delivering malware. If you don't know exactly what it is, don't click on it.

Double-check your downloads. From pirating sites to official storefronts, malware is often lurking just around the corner. So before downloading, always double-check that the provider is trustworthy by carefully reading reviews and comments.

Get an ad-blocker. Malvertising – where hackers use infected banners or pop-up ads to infect your device – is on the rise. You can't know which ads are bad: so it's safer to just block them all with a reliable ad-blocker.

Careful where you browse. Malware can be found anywhere, but it's most common in websites with poor backend security, like small, local websites. If you stick to large, reputable sites, you severely reduce your risk of encountering malware.

Unfortunately, even if you follow the above advice to the letter, you might still get infected with malware: hackers have found ways to sneak their viruses into every corner of the web.

For real security, you need to combine healthy online habits with powerful and reliable anti-malware software, like AVG AntiVirus FREE, which detects and stops malware before it infects your PC, Mac, or mobile device.

4.4 Comparative analysis McAfee vs AVG

McAfee and AVG two the best antivirus packages available. McAfee is comprehensive security, McAfee shredder and multi-faceted privacy protection. AVG is password protection, data shredder and enhanced firewall. Both have their pros and cons, and offer features that will have varying benefits to each individual user.

Antivirus software offers an array of different features.

McAfee has next functions:

1) Antivirus,
2) Security Experts and Online Support,
3) Multi-Device Compatibility,
4) Performance Optimization,
5) Home Network Security,
6) Password Manager,
7) Safe Web Browsing,
8) File Shredder,

9) Encrypted Storage,
10) Identity Theft Protection.

AVG has next functions:

1) Advanced antivirus,
2) AI detection,
3) Real-time updates,
4) Behavior shield,
5) Webcam protection,
6) Do not disturb mode,
7) Password protection,
8) Data shredder.

AV-Test examination looked at the average influence of security product on computer speed while carrying out a few common computer tasks, such as launching popular websites, installing/lunching software programs, copying files, and more. The results are displayed in terms of the slowdown a security product caused on a standard PC as well as on a high-end PC.

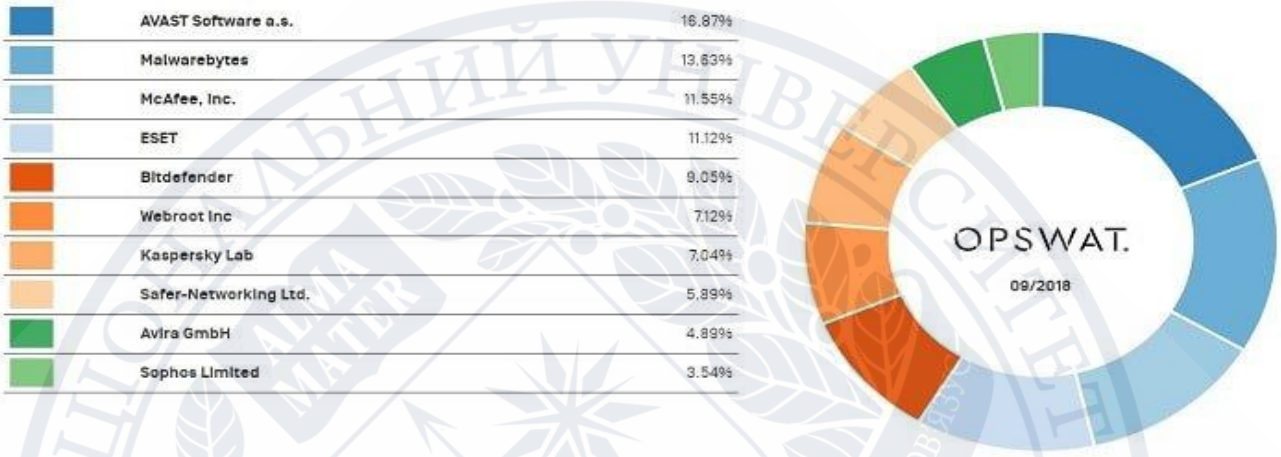
McAfee received an excellent 6/6 rating from the experts in the ‘Performance’ category [26]:

	Industry average	Standard PC	Industry average	High end PC
Slowing-down when launching popular websites 39 websites visited	15%	6%	14%	6%
Slower download of frequently-used applications 20 downloaded files	1%	1%	1%	1%
Slower launch of standard software applications 12 test cases applied	15%	7%	15%	9%
Slower installation of frequently-used applications 19 installed applications	23%	27%	22%	24%
Slower copying of files (locally and in a network) 3,687 files copied	5%	2%	10%	3%
Performance Score	6.0/6.0			

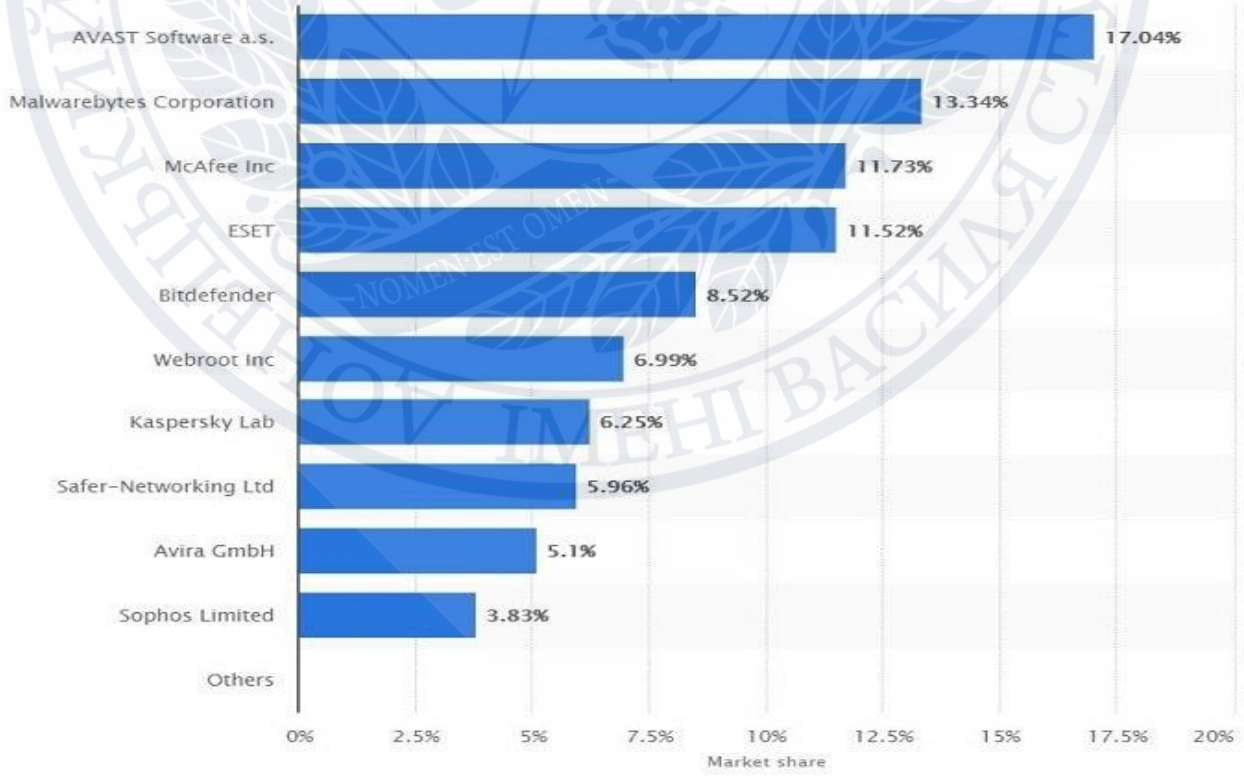
AVG, on the other hand, could only get 5.5 stars out 6 in the test [26]:

	Industry average	Standard PC	Industry average	High end PC
Slowing-down when launching popular websites 39 websites visited	15%	23%	14%	22%
Slower download of frequently-used applications 20 downloaded files	1%	2%	1%	0%
Slower launch of standard software applications 12 test cases applied	15%	14%	15%	15%
Slower installation of frequently-used applications 19 installed applications	23%	15%	22%	14%
Slower copying of files (locally and in a network) 3,687 files copied	5%	4%	10%	7%
Performance Score	5.5/6.0			

OPSWAT, which is an independent security firm, releases a monthly report on the market share of leading anti-malware products. McAfee is third on the list with 11.55% market share, while AVG doesn't make it to the list [26]:



Statista is another popular company that reports on the market share captured by leading antivirus companies. Their report is similar to OPSWAT's findings [26]:



Both McAfee and AVG provide excellent malware protection with minimal impact on system performance. But McAfee offers more protection-related features and extra utilities in its security suites than AVG.

CHAPTER 5

CONCLUSION

5.1 Summary

Let's face the reality…we are in a world where technology is advancing day after day. Generally, the computer world and the internet of things are among the fields that are evolving drastically. Although evolution in technology is something that we should embrace, it is experiencing many challenges – cybercriminals.

As technology advances, so do the cyber-criminals come up with new ways of accessing computerized devices such as PCs, mobile phones, and other devices connected to the internet. Cybersecurity is becoming more and more expensive to implement while on the other hand, cybercrimes are growing year after year.

However, some great brains have come up with the best antivirus software, which helps in protecting your devices from cybercriminals.

Moreover, antivirus help in protecting other types of attacks such as malware, ransomware, computer viruses, etc. The antivirus, whether paid or free, is essential in offering your gadgets full protection and promising you a cyber-crime open world.

You may be familiar with some terms such as McAfee, AVG, Avast, Bitdefender, Norton, and others.

5.1.1 Conclusion

In this paper we discussed about how antivirus software works. There are different ways for detecting the viruses from the system.

We conducted the comparative analysis of two biggest-selling antivirus software – McAfee and AVG.

This deep knowledge will help us to choose the best antivirus for our system so that we can provide an efficient security for our PC.

REFERENCE

[1] lifehacker: The Difference Between Antivirus and Anti-Malware (and Which to Use)

[2] “What is antivirus software?”. Microsoft.

[3] John von Neumann: “Theory of self-reproducing automata”(1949)

[4] Thomas Chen, Jean-Marc Robert (2004). “The Evolution of Viruses and Worms”. Retrieved 2009-02-16.

[5] From the first email to the first YouTube video: a definitive internet history. Tom Meltzer and Sarah Phillips. The Guardian. 23 October 2009

[6] IEEE Annals of the History of Computing, Volumes 27-28. IEEE Computer Society, 2005. 74. Retrieved from Google Books on 13 May 2011. "[...]from one machine to another led to experimentation with the Creeper program, which became the world’s first computer worm: a computation that used the network to recreate itself on another node, and spread from node to node.”

[7] John Metcalf (2014). “Core War: Creeper & Reaper”. Retrieved 2014-05-01.

[8] Creeper - The Virus Encyclopedia

[9] What was the First Antivirus Software?

[10] “Elk Cloner”. Retrieved 2010-12-10.

[11] “Top 10 Computer Viruses: No. 10 - Elk Cloner”. Retrieved 2010-12-10.

[12] “List of Computer Viruses Developed in 1980s”. Retrieved 2010-12-10.

[13] Fred Cohen: “Computer Viruses – Theory and Experiments” (1983)

[14] Fred Cohen 1988 “On the implications of Computer Viruses and Methods of Defense”

[15] Péter Ször: “The Art of Computer Virus Research and Defense” (2005)

[16] VirusBulletin: “In memoriam: Péter Ször 1970-2013”(2013)

[17] History of viruses

[18] Leyden, John (January 19, 2006). “PC virus celebrates 20th birthday”. The Register. Retrieved March 21, 2011.

[19] Panda Security (April 2004). "(II) Evolution of computer viruses”. Archived from the original on 2 August 2009. Retrieved 2009-06-20.

[20] Christodorescu, Mihai, et al. Malware normalization. University of Wisconsin-Madison Department of Computer Sciences, 2005.

[21] McGraw, Gary, and Greg Morrisett. "Attacking malicious code: A report to the infosec research council." IEEE software 17, no. 5 (2000): 33-41.

[22] Vasudevan, Amit, and Ramesh Yerraballi. "Cobra: Fine-grained malware analysis using stealth localized-executions." In 2006 IEEE Symposium on Security and Privacy (S&P'06), pp. 15-pp. IEEE, 2006.

[23] Aycock J. Computer viruses and malware. Springer Science & Business Media; 2006 Sep 19.

[25] Skoudis, E. and Zeltser, L., 2004. Malware: Fighting malicious code. Prentice Hall Professional

[24] Karim ME, Walenstein A, Lakhotia A, Parida L. Malware phylogeny generation using permutations of code. Journal in Computer Virology. 2005 Nov 1;1(1-2):13-23

[25] Canali, Davide, Andrea Lanzi, Davide Balzarotti, Christopher Kruegel, Mihai Christodorescu, and Engin Kirda. "A quantitative study of accuracy in system call-based malware detection." In Proceedings of the 2012 International Symposium on Software Testing and Analysis, pp. 122-132. 2012.

[26] Electronic resource: https://www.proficientblogging.com/mcafee-vs-avg/

ACKNOWLEDGEMENT

My first gratitude goes to the Almighty God for his protection, knowledge and understanding for seeing me through this work and the school.

I also appreciate my supervisor, Mrs. Maryna J. Iepik. I say, God bless you very much for your time, patience, directions and corrections you made in this project to make it a successful one. Thank you very much.

I would like to extend my appreciation to all the academic and administrative staff of the department of computer science and information technology

Finally, my distinct thanks go to the whole Asamoah's family for their encouragement and care.

HARRISON ASAMOAH

Family name, First name

Information and applied technologies

Faculty

122 Computer science

Code and speciality name

Computer science

Educational program

DECLARATION

I hereby declare that Bachelor's thesis «ANTIVIRUS SOFTWARE VERSUS MALWARE» is the results of my own original work, except for reference to the work of others which have been duly acknowledge.

Declare, that this work:

- that no part of the work has been presented for another degree in the university or elsewhere;
- does not violate author and contiguous rights, which fastened of articles of a 21-25 Ukraine Law «ON COPYRIGHT AND RELATED RIGHTS»;
- data and information were not got in illegal method.

I realize that in the case of violation of this order my bachelor's thesis will be declined without a right for its defense, or I get bad point during bachelor's thesis defense.

_____

Date and student's signature