HÖGSKOLAN HALMSTAD

DEGREE THESIS

Anti-Virus Programs Evaluation

Network project

2012 12

Author: Christoffer Frost

Author: Peter Månsson

Supervisor: Olga Torstensson

Examiner: Malin Bornhager

School of Information Science, Computer and Electrical Engineering
Halmstad University
PO Box 823, SE-301 18 HALMSTAD, Sweden

Preface

It has been a very interesting course and we had a lot of fun doing this project.

To our supervisor Olga Torstensson that gave us advice and feedback on our project.

To Thomas Frost who also gave good advice and feedback on our project.

Abstract

Malware is always growing and changing as new kinds of viruses and other malicious software is developed to infect and bring havoc into your computer. In an environment where almost the entire world is computer-driven, this is extra important to know.

Our report concerned malware and it's abilities to infect computer devices in different ways.

We approached this by doing a theoretical investigation on malware and testing different free anti-virus programs.

Our results was that there can be big differences in how good an anti-virus program is in terms of performance and if they actually find viruses or not, so it's important to make a good choice.

Table of Contents

Introduction

The goal of this project is to learn more about malware, and how it affects computers, how to protect yourself against it, how to remove it from your computer, and what happens if your computer gets infected.

Malware is the generic name for all malicious software. Malware is very important in todays network design and network planning. Malicious software is a big problem in todays networks because their sole objective is to bring havoc into the network in different forms. It consists of five main parts: viruses, worms, trojan horses, adware and spyware.

A virus is a piece of code or a small size software that "hitchhikes" on another program, so when you start the original program, the virus starts too. Each time you run the program, you run the virus that will try to ruin your computer or reproduce itself to make an even bigger disaster.

A worm is like a virus, but it focuses on infecting the entire network rather than just the host computer. It finds holes in the security of the network to always find somewhere new to reproduce and spread further.

A trojan horse does not replicate automatically. It sets out to be a program, like a video file but in fact it is a malicious program that for example removes crucial windows files [1].

Adware is an application that makes ads pop up on your screen, making it hard to use the computer properly.

Spyware is a program such as a keylogger that runs in the background and tries to steal important personal information, such as your credit card number or your passwords [2].

On July 19th 2001 the worm known as Code Red Worm infected more than 359,000 computers in less than 14 hours. The 20th of July the worm was programmed to make all the infected machines do a denial-of-service attack on the White House webpage [3, 4].

A denial-of-service attack means that the target is getting alot of requestes, more than the internet link can handle and the people trying to access the webpage will be unable to do so, or there will be a very long response time. If servers becomes unreachable workers are unable to access them and work towards them.

The purpose of this report is to give insight into what malware is, focusing on viruses, worms, trojan horse, spyware and adware, which are the five biggest pieces of Malware.

We chose malware as a subject because we think it's a relevant subject, which we also think is interesting to write about. We want to learn more about it, and pass it on to others.

Malware can affect the society in many ways. If you get infected with malware in a home environment it can have a lot of different outcomes. It can be as mild as editing your word document or as severe as stealing your banking information. If an enterprise gets infected by for example a harmful worm, it can make a lot of damage and make the enterprise lose a lot of money due to the employees not being able to work.

If the servers that handles the train ticket machine gets infected, people will most likely be unable to buy train tickets. It could also be for example an office environment, where the IT-technicians have a lot to do but are forced to spend time solving malware issues instead of other things. With good anti-virus implementation, these risks will be drastically reduced.

It's hard to get a good example on how malware affects the environment, but an extreme example could be if a water treatment plant got infected that would result in getting dirty water in the society. Another example could be if a system for traffic lights in major cities got infected, which could result in car crashes.

There is also some other ethical consequences. Stealing personal things like personal photos or videos that people keep in their computer is another example, or stealing money from someones bank account.

Method

We want to describe what malware is, and give examples of different kinds of viruses, worms, trojan horses, spyware and adware. We also want to describe how to protect yourself and what to do if you get infected.

After that we will infect a newly formatted, fully updated Windows 7 PC with a test-virus called eicar, which is used for testing if your anti-virus software will detect malicious software and how it reacts to it. We will test four different free anti-virus programs. The reason for this is because anti-virus software tends to be pricy. We will test downloading the test-virus in multiple ways: as a normal .exe file, in compressed files such as .zip and double .zip. We will lastly scan the computer with each anti-virus software and see what happens when it finds a malicious file.

The reason we chose to go with eicar is that it is recommended by multiple big anti-virus companies, such as McAfee and F-Secure, in order to test your anti-virus programs functionality [5, 6]. Eicar is solely created for one reason: to test the functionality of your anti-virus program.

We focused at both doing a theoretical investigation and a practical implementation. We also prepared by doing a time plan and doing internet research on different free anti-virus software that we put in a list, from which we then chose which programs we wanted to test. We also spent some time looking for a test-virus that we could use to test the different anti-virus programs we chose. Our target group is really anyone who needs help finding a good free anti-virus program and anyone who is interested in IT-security and malware.

We found all our information regarding the theoretical background on the internet, and we made sure the sites were legitimate with people that had worked a lot with these subjects.

The first step of the practical implementation was to put the test-virus on the desktop before we installed an anti-virus program, because our hypothesis was that the anti-virus programs would stop us from downloading the test-virus to begin with, so we tried to download it with the anti-virus program activated to try our hypothesis. As expected, we were not allowed to download the test-virus, so we did have to deactivate the anti-virus programs in order to actually be able to get the test-virus in the system for further testing.

This was because we also wanted to see how the software reacted when we scanned the system and a malicious file was found. After that we installed the first anti-virus program. We then tried to download the virus in different ways (as an .exe file, as a

.zip and double .zip) to see if it had trouble finding a virus if it was compressed. After that we scanned the computer to see how it reacted when it found malicious software. When all those steps were done, we did the same with a new anti-virus program. The anti-virus software we used was:

- Microsoft Security Essentials
- Avast Free Antivirus
- AVG Free Antivirus
- Panda Cloud Antivirus

The theoretical background consists of the following sections:

- Virus
- Trojan Horse
- Worm
- Spyware
- Adware

Theoretical Background

1.1 Virus

A virus is a program or a piece of code that spreads by the use of other, normal programs, documents or other files. Viruses can be spread in a number of ways, such as an attachment in an e-mail or in a file that you download from the internet. Viruses can both start spreading havoc in your system the second you run the file they are attached to, or be dormant in your system until something makes their code get executed by the infected computer. Viruses can be very harmful and erase data or make sure your hard disk will need to be reformatted. The three main virus-classes are File infectors, System or boot-record infectors and Macro viruses [7].

The best way to protect yourself from getting a virus is to always be sure of what kind of file you are actually downloading, and this can still be hard because a file that seems legit can still be infected. You should also be careful of strange e-mails with attachments or links as they often contain viruses. You should also be careful with "virus hoaxes", which is a false warning about computer viruses that commonly comes with e-mail notes or that is distributed in the internal network of a company [8]. It is also recommended to use anti-virus software that will protect you by checking your files periodically, remove viruses that are found and even warn you when you try to enter sites known to contain infected files.

If your computer gets infected there are never one solution that fits all infections, therefore it's hard to explain what to do if you do get infected by a virus. If you are lucky you can just remove the file straight away, but sometimes you might even have to reformat your entire system.

1.1.1 File Infectors

Different file infector viruses infect different types of files (.com, .exe, .sys, .ovl, .prg, .mnu). When you run an infected file, you also start the virus. An e-mail attachment can also contain a file infector virus, in form of for example a script [7].

When a file with a virus infection is run on a system it will find other files and put its code in the files it finds. The code will be put in the beginning (prepending viruses), end (appending viruses) or middle (mid-infector viruses) of the file. If the file have gaps in its structure, the code can also be inserted in those gaps. The entry point of the file is then re-directed to the virus, so that when the file is executed the virus is also executed [9].

1.1.2 System or Boot-Record Infectors

The system or boot-record infectors target certain areas on a disk to infect.

An example of the way these viruses works is that you receive a diskette that contains a boot disk virus. When you run files on the diskette, you can do so without activating the virus. If you keep the diskette in the drive and reboot or turn off the computer, once it boots it will first look in the A drive where the diskette is, which contains the boot disk virus, load it and from there make sure your system is infected [7].

1.1.3 Macro Viruses

Macro viruses are among the most common and the least harmful viruses. Any operating system can receive a macro virus as long as it has Microsoft Office installed. The virus attaches itself to a document and lies dormant until for example Microsoft Word opens it.

The way you get this virus is when you open a file (normally a document or a template) that has a macro virus attached to it. When you open the document the virus will be executed and spread to other documents. You can also receive a macro virus from e-mail attachments.

There are some symptoms of the macro virus. For example it can change the format in which you save your file (from .doc to .dot). If you want to "save as" it can make sure that there are only one format that is available to save the file as. It can password protect files even though you haven't put password protection on them yourself. It can also insert random words at random locations in your document and give you unusual messages when you open a file. It can even lead to e-mail applications stopping you from mailing documents since they are infected [10].

1.2 Worm

A Worm, unlike the virus contains all the code it need to carry out its purpose alone and do not need help from another program. Worms survives by reproducing themselves on the infected hosts, internet, e-mail and network. The worm can do this even without the hosts knowledge because it is usually hard to detect if the computer is infected or not. That means every host affected can send thousands of worm packages before it is detected [11, 12].

One type of computer worms are the e-mail worms, they spread themselves by sending themselves to all the infected hosts e-mail contacts in hope that some of the contact hosts will become infected as well [11].

Most anti-virus programs detect worms trying to enter the system and blocks the worm before it can enter. But a good firewall and blocking unused ports would be the best way to keep the worms out.

If the host gets infected it is usually easier for it to spread around inside the network and it will be hard to eliminate, but trying to isolate it as fast as possible and use anti-virus programs to remove it is the best chance.

1.2.1 Payload

Payload is an option to the worms, it is not necessary but some worms are programmed for secondary tasks (the primary is to reproduce), whereas the secondary task might be anything. One common payload are to use the infected hosts as bots. The bots can be used for spamming for example a website to create a lot of requests and reduce the quality and performance of that websites server. Some worms without a payload might just be someone testing how fast the worm can spread.

Some worms actually have a good intent, and tries to secure the hosts vulnerabilities, often the very same one the worm used to enter the system. An example is if you find a bug in windows for example, you can create a worm that exploits that bug to get inside the computer of others and from there it will secure that bug so that others might not exploit it [13].

1.3 Trojan Horse

The trojan horse is named after the greek mythology, where the greeks presented a big wooden horse as a gift to the citizens of Troy. They opened their gate and took the horse inside their city, but what they didn't know was that it was filled with greek warriors, whom ran out from the horse in the night, inside the city walls.

The malicious software with the same name works pretty much in the same way. It sets out to be a software or file that is harmless, but in reality when you run it you activate the harmful code inside of the file, which then proceeds to ruin your system. There are six main types of trojan horses: Remote-Access Trojans, Anti-Protection Trojans, Destructive Trojans, Data-Sending Trojans, Denial-of-Service Trojans, Proxy Trojans [14].

The best way to protect yourself from getting a trojan horse is to keep your anti-virus software updated and to be careful of running files or opening e-mail attachments if you are not fully sure that they are legitimate.

Just like with the virus, there is not one solution that fits all if you get infected by a trojan as it depends on the damage it does. Sometimes you can just remove the infected files, sometimes you might have to format your systems hard drive.

1.3.1 Remote-Access Trojans

Remote-access trojans are also called RATs or backdoor trojans and they are the most harmful and most common trojans. Typically the host doesn't notice them running on the system because they do not show up in the task managers list of programs or tasks that are running [14, 15].

It works in a way that it gives an intruder full access to the host system. It works pretty much in the same was as legitimate remote administration programs like for example Symantec's pcAnywhere [14]. Like most trojans, it is typically hidden in small .exe files. It is also common in e-mail attachments.

Once an intruder has remote administrative control of your PC he can do a number of things, such as monitor you with a keylogger or other spyware, access personal information like your credit card information and such. It can activate your webcam and start recording you. It can also format drives and download or change files on your system [15].

1.3.2 Anti-Protection Trojans

Anti-protection trojans are also called security software disablers. The reason they are called this is because they are used to disable your anti-virus software or your firewall so you more easily can be attacked by an intruder [17].

1.3.3 Destructive Trojans

Destructive trojans have one sole purpose, and that is to delete your files. They can automatically erase all of the most important system files (.dll, .exe, .ini files) on the host PC, and it can either be activated by a hacker or lie dormant until a certain date or time [16].

1.3.4 Data-Sending Trojans

Data-sending trojans sends personal data to the hacker like for example passwords or banking information. It can either search for this information in certain places of the harddrive or install a keylogger and send the keystrokes to the hacker [14].

1.3.5 Denial-of-Service Trojans

Denial-of-service trojans works in a way that it infects multiple computers with a zombie that has a scheduled time where it will attack a certain website at the same time. The high traffic from all the computers attacking it at the same time will cause

the web servers to be inaccessible, making the website slow or impossible to load [14].

1.3.6 Proxy Trojans

A proxy trojan will turn an infected computer into a proxy server. This proxy server is then used for the attacker to provide anonymity for things like buying things on the internet with a stolen credit card or performing denial-of-service attacks. If you go through a proxy server when you do this, it means that when the actions are tracked, the trace will lead to the proxy server and not the actual hacker [14].

1.3.7 Zeus Trojan (Zbot)

Zeus is a malware toolkit that makes you able to build your own trojan horse. Zeus is a software that is sold on the black market and can cost between 3000 USD and 10000 USD depending on what kind of modules you will use.

Once the unsuspicious computer have been infected with the Zeus trojan it wil lie dormant until the user decides to visit a web page which contains a form that needs to be filled out. Zeus has a very nasty feature which allows the hackers to add fields on the already existing web site forms. So instead of re-directing the user to another website then the one he/she originally wanted to join, there is instead extra forms to fill in on the original web site. It is often used for stealing personal online bank information [16].

1.4 Spyware

Spyware is software that makes an attacker able to gather information about yourself or your organization without you knowing about it [17]. There are five main types of spyware: adware, keyloggers, modem hijackers, browser hijackers and commercial spyware [18].

The best way to protect yourself from getting spyware is to be careful with what files you download and what e-mail attachments you open.

Just like with the virus and trojan horse, there is not one solution that fits all if you get infected with spyware. Sometimes you can go into your registry and remove it, sometimes you may have to re-format your computer.

1.4.1 Keyboard Logger

Keyboard loggers, also known as keyloggers, is malicious software. Its purpose is to steal information such as PIN codes, credit card numbers or passwords by logging the key strokes you make and sending it to the hacker [18].

1.4.2 Modem Hijacker

Modem hijackers ties into your phone line to make calls and access web sites without your knowledge, often ones that cost money [18].

1.4.3 Browser Hijacker

Browser hijackers targets your internet access through resetting things like your bookmarks and your homepage. It then tries to direct you to counterfeit sites with for example spam advertisements. These softwares can also record what web sites you are browse and give this information away to other people [18].

1.4.4 Commercial Spyware

Commercial spyware is not intended to be harmful but rather an agreement you make with companies. In order to get free software or access free social networks they might require you to let them monitor you with a form of spyware. Through this spyware they will then send you advertisements when you use their software or social network [18].

1.4.5 TIBS Dialer

The TIBS Dialer is a form of modem hijacker. It installs itself via spam e-mail attachments or when you are browsing certain web sites. It then hijacks your modem and starts dialing phone numbers that access porn sites you have to pay for. It does not affect the performance of the PC and the only thing you most likely will notice from it is a big telephone bill. As if that wasn't enough, the TIBS dialer will also show porn advertisements on your PC and even connect to the Internet where it tries to access paid websites. [19].

1.5 Adware

Advertising-supported software is a software that integrates itself into the host system and takes over a toolbar or the web browser. If the web browser is taken over it will still work but sometimes when visiting pages there will be pop-ups or it may redirect the browser to another page then the user intended [20, 21].

Adware infects the computer buy being installed together with a freeware program. A freeware program is a free software and it may do anything from adding a search bar in your web browser to being a new browser itself [20, 21].

Adware also collects information about the user, statistics so that it can display commercials most relevant to the user. The way the adware does this is by creating a user profile where it saves web browser history. Sometimes the adware might save more information than just web history to be able to display the most relevant ad,

sometimes it saves computer preferences, and as much information as possible about the user that may later be sold to third party. Usually when downloading freeware the user can read about where the information go and what information is collected in the user agreement, but not always [20, 21].

Not all adware is malicious, for some web developers it's a way to get money, by putting an advertiser on the webpage they can allow companies to pay for their commercial to be displayed on the webpage [20, 21].

The easiest way to protect the computer from adware is to read user agreement when downloading freeware. Also avoid clicking on "You have won!" adds on webpages.

If the computer gets infected you could try to remove the software the adware came from or use an anti-adware program, but that might go against the user agreement of the software that infected you with the adware.

2 Practical Implementation and Results

As our practical implementation we focused free anti-virus software.

2.1 Parameters

When we test the tools, we will be looking at different parameters to judge how well they are working. Things such as how user-friendly the tool is to use, or how much strain it puts on the CPU is just a few things that can be important to know when you choose a anti-virus program. To determine the performance, we chose to use these parameters:

- Size
- Idle CPU usage
- Idle RAM usage
- Active CPU usage
- Active RAM usage
- If it was able to detect and remove the viruses

We will also look at user-friendliness, complexity and special features.

2.2 Test Computer Specifications

We used a freshly formatted, fully updated computer with the following specifications:

- Windows 7 32 bit
- AMD Athlon 64x2 Dual Core 2.6GHz
- 4GB RAM
- Radeon x1600
- Maxtor 6y 200p0 500GB

2.3 Anti-Virus Programs

There were four different anti-virus programs tested. We chose those programs because they were free and popular, so the chance of someone using those programs

are bigger since there is a lesser chance of someone using an anti-virus program that isn't popular. Since the goal with the project was to test free anti-virus software in home environments, we felt like these were the best choices:

Microsoft Security Essentials

Avast Free Antivirus

AVG Free Antivirus

Panda Cloud Antivirus

To test each of the programs there was a malicious file planted in the system and also different malicious files that we tried to download. The file is called eicar, and we tried to download it as .exe, .zip and double .zip, since compressed files are harder to detect.

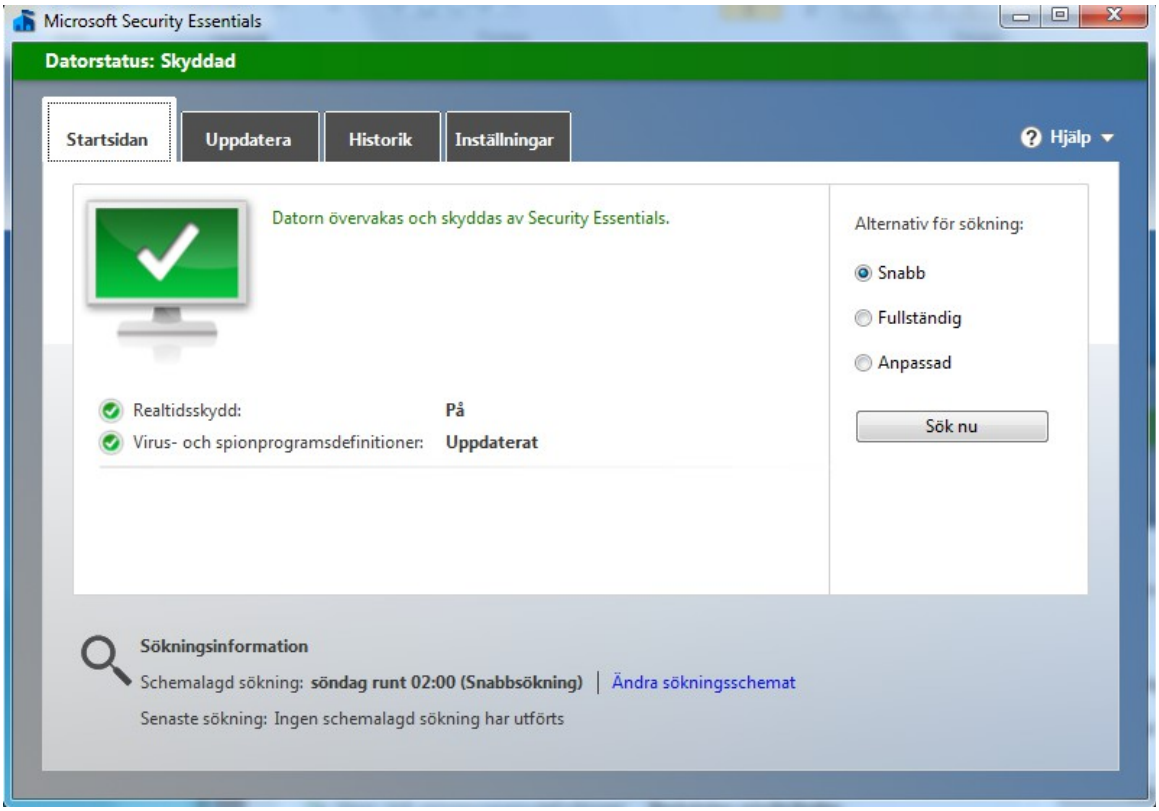
2.3.1 Microsoft Security Essentials

A table of parameters of Microsoft Security Essentials can be seen below.

Paramater	Value
Size	21.8MB
Idle CPU usage (not scanning)	3-5%
Idle RAM usage (not scanning)	22,00%
CPU usage (scanning)	50,00% (since this was the default limit. If we would have chosen 20% limit, thats how much it would had used).
RAM usage (scanning)	28,00%
Able to detect malware	Yes

Table 1-1 Microsoft Security Essentials

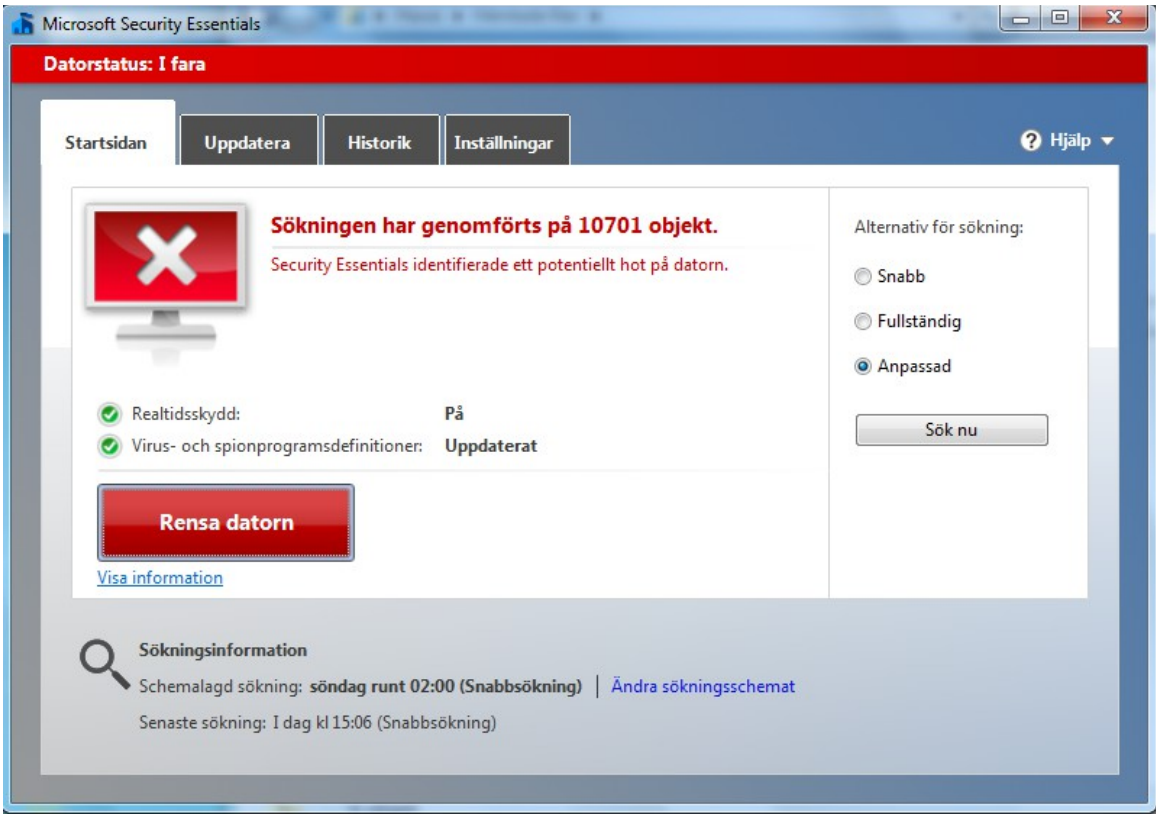
We then started the program, and the first thing that hit us was that the interface felt user-friendly. We included a picture of the starting window (in swedish) as seen in picture 1-1 below.



Picture 1-1 Microsoft Security Essentials starting window

We then had a look at the settings and options of Microsoft Security Essentials, and there was two things in particular that was interesting. The first thing was the ability to schedule scans so that you could choose a day and time to perform the scan. The second thing was the ability to limit the amount of CPU power that was to be used for scanning the system (the default was 50% CPU power), which is neat if you have a weak computer.

A thing to note is that if you scanned the system and it did not contain a virus, you would not get a report after the scan was finished. However, when the system did contain a virus, we received a report, as seen in picture 1-2 below.



Picture 1-2 Microsoft Security Essentials detecting a malicious file after a scan

The popup from the anti-virus program when you tried to download a malicious file was small and it did not really catch your eye. It was also green which is quite odd, as the color green normally indicates that something is secure.

When we tried to download the test-virus in different ways, it detected and easily removed it, wether it was .exe, .zip or double .zip.

2.3.2 Avast Free Antivirus

A table of parameters of Avast Free Antivirus:

Parameter	Value
Size	325MB
Idle CPU usage (not scanning)	1-2%
Idle RAM usage (not scanning)	31,00%
CPU usage (scanning)	8,00%
RAM usage (scanning)	31,00%
Able to detect malware	Yes

Table 2-1 Avast Free Antivirus

You could schedule scans to different days and times, just like you could in Microsoft Security Essentials. Picture 2-1 below shows the summary screen of Avast Free Antivirus.

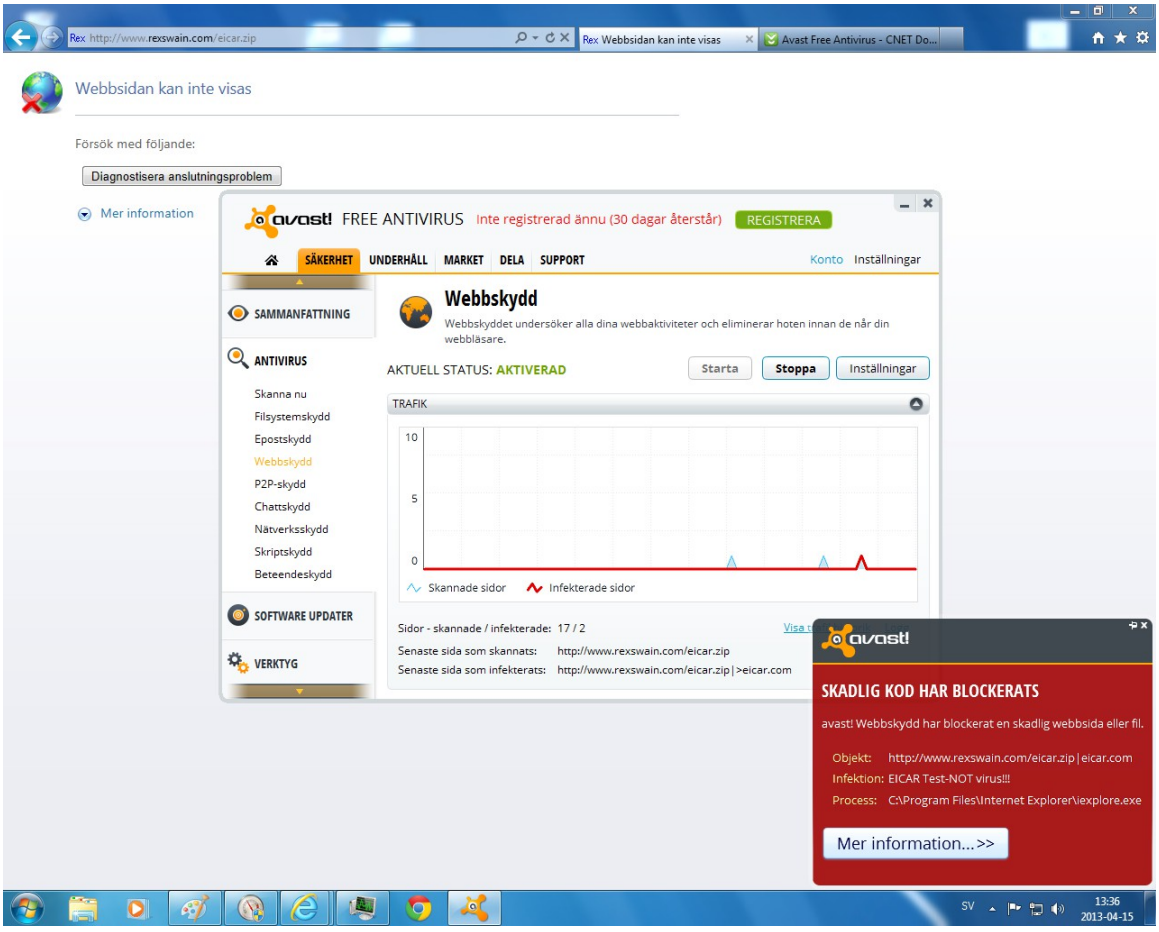
Picture 2-1 Avast Free Antivirus summary window

The user interface however, wasn't user-friendly to navigate in. But, when you had found what you were looking for, the interface was nice and gave you a lot of information.

A good feature that Avast Free Antivirus had was called Software Updater. What it did was to check certain applications – such as web browser – and made sure that they were updated to the latest versions. This is because older versions might have security holes in them.

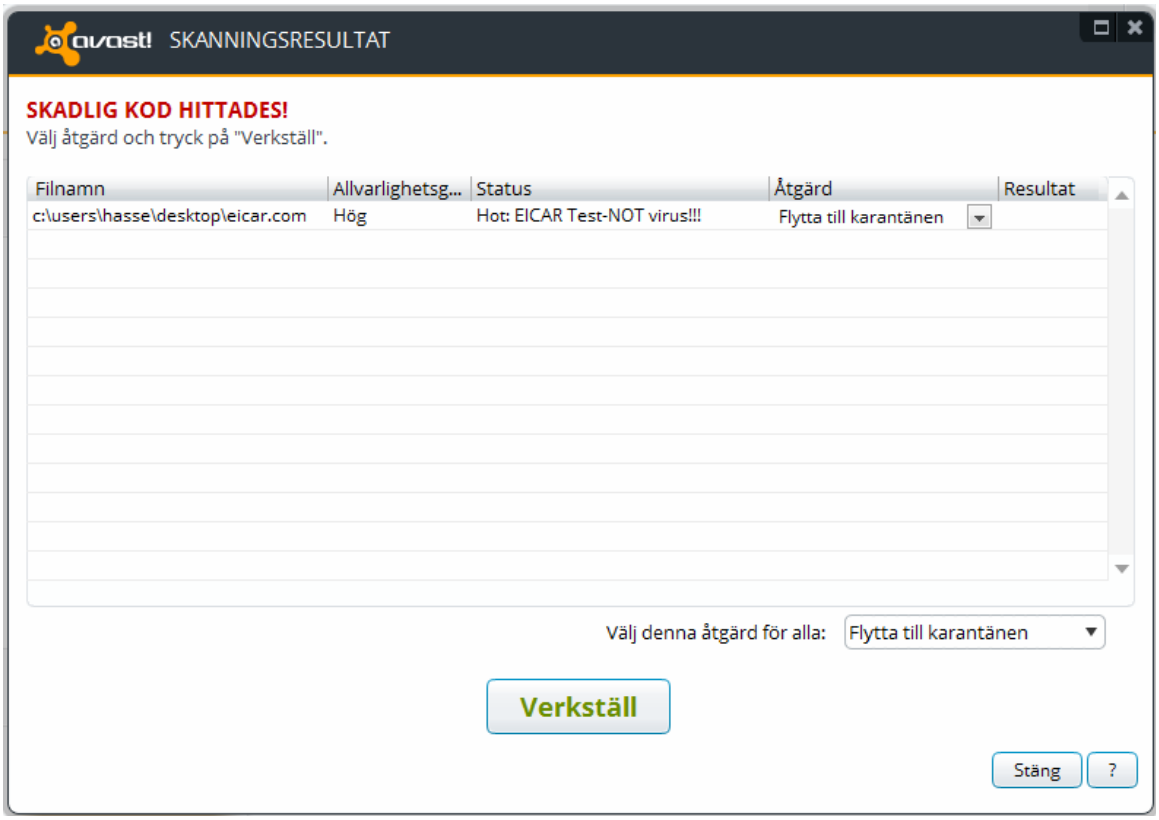
After a completed scan (with and without a virus file) you got a good scan report containing information such as: how many files that were searched, how many of those were infected, how long the scan took and how many MB of data that was searched.

When you tried to download the test-virus, you got a big, red and easy to spot popup, warning you that the file contained a virus. Another good feature it had was to put an error message on the website you were visiting so you could not keep accidentally browsing it. Picture 2-2 below shows Avast Free Antivirus detecting when we tried to download a virus.



Picture 2-2 Avast Free Antivirus detecting a download of a malicious file

We tried to download the test-virus eicar in different ways with this anti-virus program as well, but it detected and easily removed all the different test-virus files (.exe, .zip or double .zip).



The last thing we did was to scan the system in order to see if it would find the virus that we had planted, which it did as you can see in picture 2-3 below.

Picture 2-3 A completed system scan with Avast Free Antivirus

2.3.3 AVG Free Antivirus

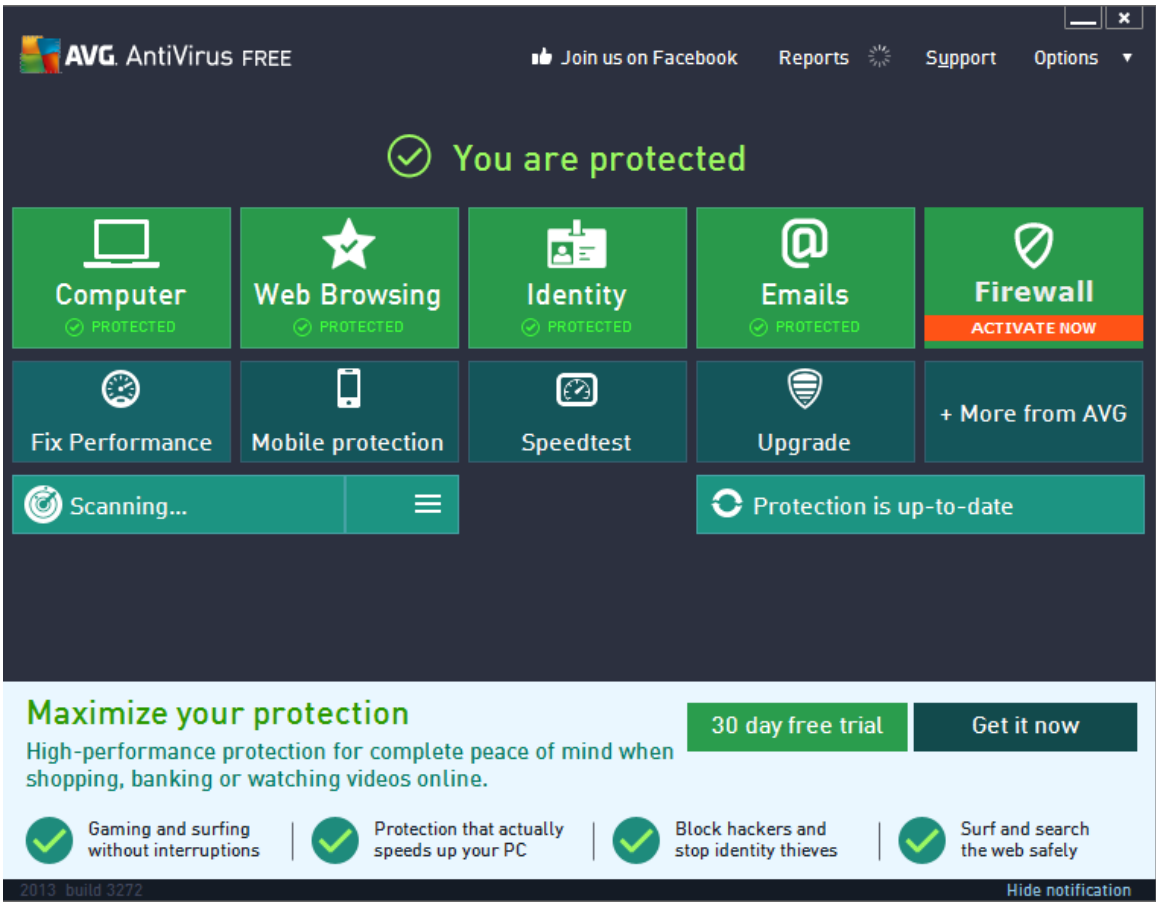
Below is a table of parameters of AVG Free Antivirus:

Parameter	Value
Size	84.3MB
Idle CPU usage (not scanning)	3,00%
Idle RAM usage (not scanning)	29,00%
CPU usage (scanning)	35,00%

RAM usage (scanning)	29,00%
Able to detect malware	Yes

Table 3-1 AVG Free Antivirus

The interface was user-friendly and easy to navigate in, as can be seen in picture 3-1 below.



Picture 3-1 The starting screen of AVG Free Antivirus

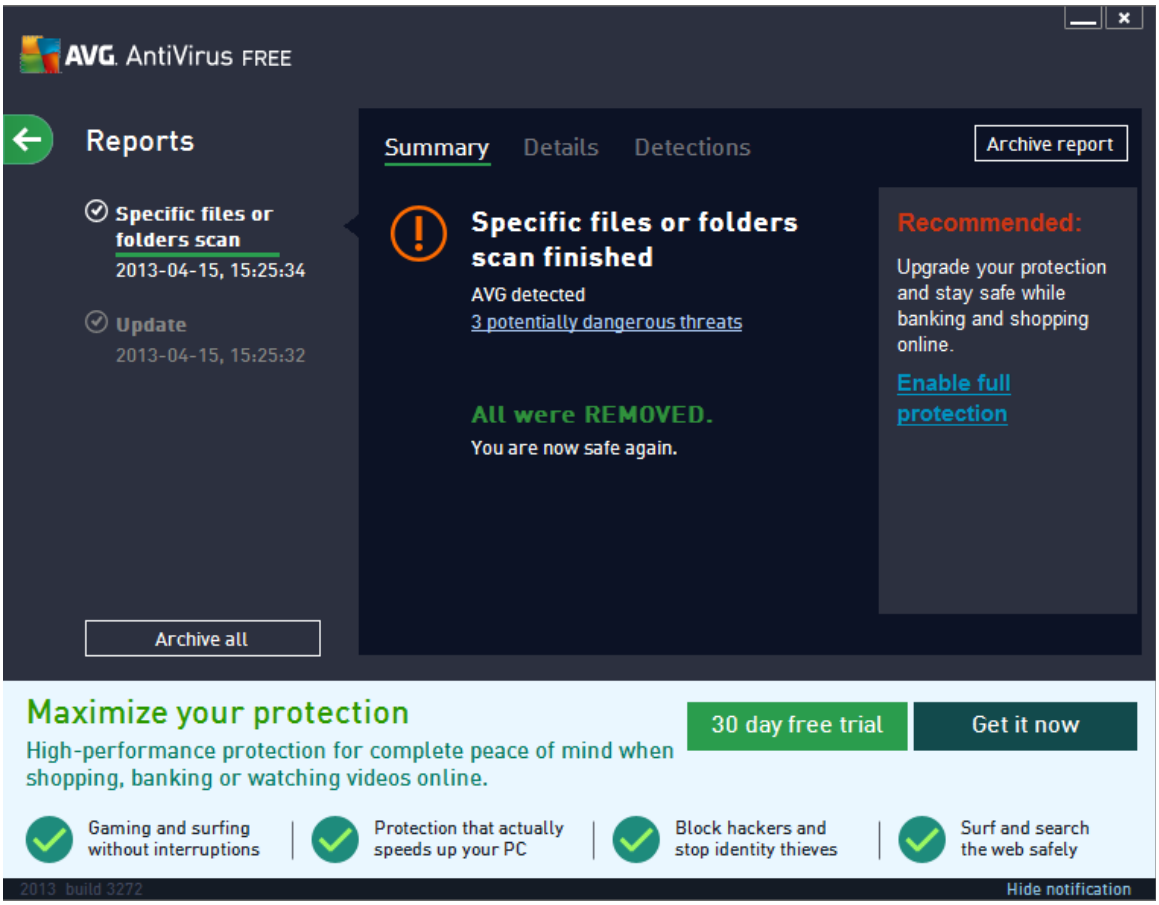
AVG Free Antivirus also contained scheduled scans. The scan reports contained a lot of information. It had an "optimization" feature, which meant that it would scan the system and remove any unnecessary files, such as temporary files and web history. It had a good popup window that appeared in the middle of the screen, which had a good feature: if you knew the source could be trusted, you could choose to ignore the threat instead of protecting yourself, which none of the other anti-virus programs we tested would allow, as shown in picture 3-2 below.

Picture 3-2 AVG Free Antivirus detecting a threat

AVG Free Antivirus did not have the ability to quick scan the system. You could instead choose wether to scan the whole system or if you wanted it to scan particular files or folders.

When we tested AVG Free Antivirus by downloading eicar, the test-virus, we came across something worrying. While it would find the test-virus when we downloaded it as .exe, it would not detect the virus if it was .zip or double .zip until we actually opened the folder. This means that we could save the folder on the desktop and not know that we had a virus in our system. When we opened the compressed folder however, it did detect the malicious file.

Lastly we scanned the system to see if it would detect the virus, which it did without problems, as can be seen in picture 3-3 below.



Picture 3-3 AVG Free Antivirus after a finished scan when it detects a virus

2.3.4 Panda Cloud Antivirus

Here is a table of parameters of Panda Cloud Antivirus:

Parameter	Value
Size	97.0MB
Idle CPU usage (not scanning)	3,00%
Idle RAM usage (not scanning)	17,00%
CPU usage (scanning)	10,00%
RAM usage (scanning)	25,00%
Able to detect malware	Yes

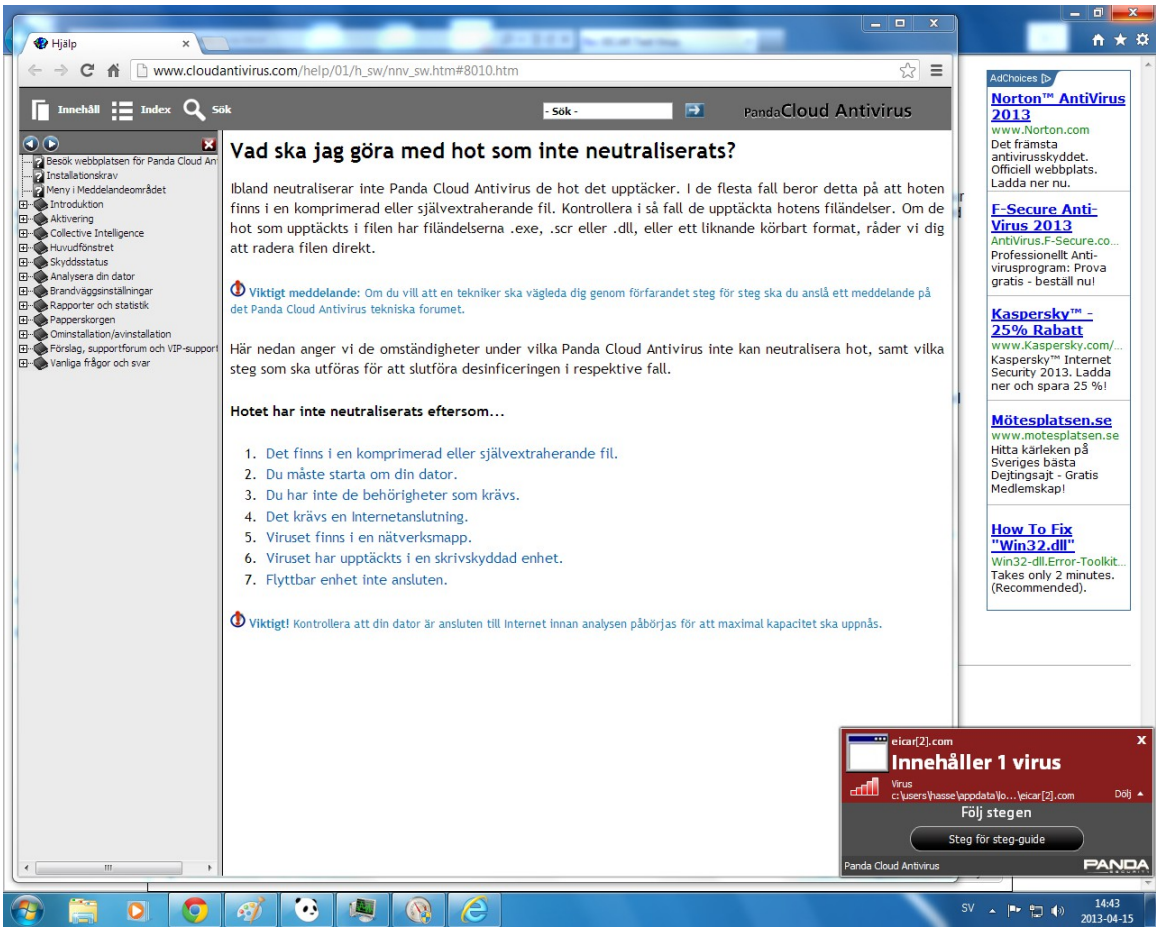
Table 4-1 Panda Cloud Antivirus

The interface was messy and also had terms you're not used to seeing. An example was that they used "Analyze" instead of "Scan", which can be confusing to many

people, when you want to scan your system for a virus. It was hard to navigate in the software and it was not user friendly at all. It was also difficult to configure, because the configuration-window was just a long list of options without any kind of structure. Picture 4-1 below shows Panda Cloud Antivirus' starting screen.

Picture 4-1 Panda Cloud Antivirus starting screen

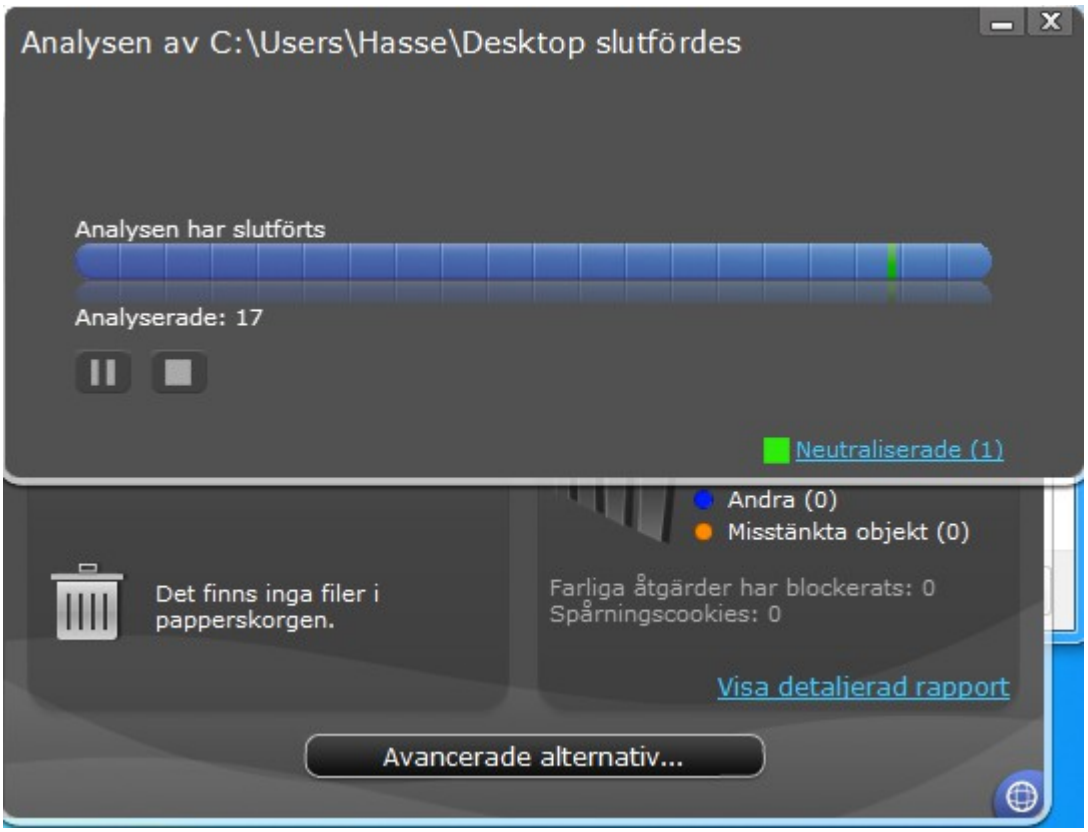
When we decided to test the anti-virus we noticed something worrying. It worked fine to block and remove a virus when it was just a simple .exe file, but we started having problems when we tried to download it as .zip. It did detect that the file contained a virus, but it was unable to remove the file, and in order to remove the malicious file you had to do a manual step-by-step process from a window that Panda Cloud Antivirus opened. According to picture 4-2 below, Panda Cloud is actually unable to remove malicious files that are contained in a .zip format! It also did not block us from downloading the file if we wanted to.



Picture 4-2 Panda Cloud Antivirus' step-by-step process to remove threats

The last test was as usual to download the file as a double .zip. Panda Cloud did not even detect that the file contained a virus and we could happily download it and save it on our system. When we then did open the compressed folder containing the malicious file, we got a warning.

The very last thing we did was to use the Analyze (scan) feature to see if it would detect a virus on the system, which it did, see picture 4-3.



Picture 4-3 Panda Cloud Antivirus after a completed scan

3 Result and Analysis

Three out of the four anti-virus programs we used were available in Swedish, which is good seeing as there are people that does not understand English.

All the anti-virus programs had the ability to perform scheduled scans, which is a good thing if you regularly want to test your system.

Basically, if you choose the right anti-virus it is definatly good enough for your home-environment or home office.

User-friendliness and complexity is our personal reflections and does not have to be the same for everyone. We checked for how many buttons there was, the level of technical language used, the depth of the different settings, how many settings there was, and how easy or difficult it was to navigate in the program.

3.1 Microsoft Security Essentials

Microsoft Security Essentials was the first program we tested, and together with Avast we think this was the best one. To begin with, its filesize was only 21.8MB which is very little. Its performance was also very good, both idle and active.

The fact that you could choose how much of the CPU power you wanted to use at maximum during scans was a very good feature which we have not seen with any other anti-virus software.

It was simple, clear and fresh. Very user-friendly and a good interface. It was also a Microsoft product which meant it worked well with Windows.

It excelled at the tests we performed and detected and removed all the malicious files we tried to download, as well as finding malicious files on the system when we performed a scan.

The only bad thing we can come up with was the fact that the pop-ups when we tried to download a file were small and green. Ideally we would like them to be a bit bigger and red, because the color green does not signal "danger", which red does.

We used the following parameters to test the program:

It easily detected and removed viruses in different forms (.exe, .zip, double .zip.)

After that we looked at the complexity of the program. It had many different settings, but was easy to understand and set up, which means it was not very complex. It had some special features as well. You could limit how much of the CPU you wanted to use for scanning the system which was very nice. You could also schedule scans for different times.

3.2 Avast Free Antivirus

Avast Free Antivirus was together with Microsoft Security Essentials the best anti-virus program. It removed all the threats we tried to download without any issues and it also found the malicious file saved on the system when we performed a scan.

The performance of Avast Free Antivirus was good, both when it was idle and scanning.

It had a feature called Software Updater which we haven't seen in the other programs. It keeps certain software – such as web browsers – up to date by always making sure you have the latest version downloaded and installed because the older versions contains security holes.

When you tried to download a malicious file it had yet another very good feature, which was that it blocked the site you were using, preventing you from accidentally keeping on browsing it since it contained threats to your system.

At the first glance, the interface of Avast Free Antivirus looked messy and hard to navigate in, but when you started using it, it was not that bad and navigating was actually very easy.

Compared to the other programs we tested, this was by far the largest filesize, with a total of 325MB.

It detected and removed all malicious files.

After that we looked at the programs complexity. It was a bit complicated and many settings you could have a look at to tweak the program as you wanted it. It also had some special features. There was a feature called program updater which would see if software such as your web browser was up to date in order to use the exploit of security-holes. It also had scheduled scans so you could plan out scans in advance.

3.3 AVG Free Antivirus

AVG Free Antivirus was the third best anti-virus program we tried. We would not recommend this program but not because we think it was bad – because it wasn't – but because we think that you should have a program that completed every part of our test, which this didn't.

It was very user friendly and had a great pop-up when we tried to download a malicious file. It also gave you the option to ignore the threat to your system when you downloaded a file, if you knew the file was safe but the program did not.

AVG Free Antivirus had a feature that could optimize your system and remove old Windows-files, repair the system, remove temporary files and other similar things, which we did not find in any other anti-virus program.

Sadly, AVG Free Antivirus did not detect .zip files or double .zip files when you downloaded them. Once you opened the compressed folder containing the malicious file you got the warning, but by then it can be too late.

It was able to detect and remove .exe files, but .zip and double .zip files were not detected until you opened the folder. It was able to remove all files once it found them.

We then looked at the complexity of AVG. It was not complicated at all, easy to change settings to your needs and easily navigated in. We then moved on to its special features. It could optimize the system, which means it removed unnecessary temporary files, clear the web history and remove cookies, for example. It also had scheduled scans which allows you to plan scans for the future, or for regular use, such as scanning every wednesday night at 01:00. Additionally you could chose to ignore a threat, which means that if you know that a file is safe but it appears to be unsafe, you can choose to ignore the threat and continue using it.

3.4 Panda Cloud Antivirus

Panda Cloud Antivirus was without a shadow of a doubt the worst of the programs we tested. We do not recommend this to anyone. The only good thing we could find about it was that it did not take up much of the computers performance.

The interface was incredibly messy and hard to navigate in. It used terms you are not used to seeing when you use anti-virus programs, such as "analyze" instead of "scan". It might not seem like much, but it can confuse you a lot.

It did detect and remove the malicious file when it was in .exe format. But when we tried to download it as .zip and double .zip, it got very worrying. It did detect that the .zip file contained a virus, but it was unable to remove compressed files. The only thing Panda Cloud would do was to open a new window with a step-by-step process on how to remove compressed viruses. Needless to say, this is not a good solution, especially seeing as you may have no idea where you even saved the file to try to manually delete it.

Panda Cloud did not even detect the double .zip file until you had saved it and opened it. Yet again, it could not remove threats in compressed files, which all of the other programs could.

It detected and removed .exe files. It detected .zip, but could not remove it. It did not detect double .zip at all.

After that we looked at the complexity. Setting up the program was difficult, and you easily got lost the settings. The only special feature it had was the ability to schedule scans, if you wanted the program to do automatic scans at any point in time in the future.

5.5 Comparison

Antivirus Program	Microsoft Security Essentials	Avast Free Antivirus	AVG free antivirus	Panda cloud antivirus
Size	21.8MB	325MB	84.3MB	97MB
Idle CPU	3-5%	1-2%	3,00%	3,00%
Idle RAM	22,00%	31,00%	29,00%	17,00%
Active CPU	50,00%	8,00%	35,00%	10,00%
Active RAM	28,00%	31,00%	29,00%	25,00%
Able to detect malware	Yes	Yes	Yes	Yes

9-1 Comparison table

As you can see in the table above, the programs vary greatly in size. The largest program being 325MB, while the smallest is 21.8MB. The programs did not affect the CPU much while being idle on the computer. However, when they were active in scanning the system, they did vary a lot.

There was a slight variation in the idle RAM usage as well as when it was active when the software scanned the computer. Another thing we noticed is that Microsoft Security Essentials and Panda Cloud Antivirus had more RAM usage while scanning, whereas Avast Free Antivirus and AVG Free Antivirus used the same amount of RAM both when it was idle and when it was scanning the computer.

The way the programs detected malware was different. Microsoft Security Essentials and Avast Free Antivirus had no trouble detecting malware in different file formats, but AVG Free Antivirus and Panda Cloud Antivirus struggled when the malware was hidden in .zip and double .zip.

4 Conclusion

We think that a lot of people underestimate just how bad having your computer or network infected can be. Most people think that "oh, I got a virus. No big deal, I'll just try to re-format my computer", or they are just too lazy and doesn't see the seriousness in an infection, when in fact they may have spyware on their computer trying to steal their bank information.

We also think that people don't always notice that their device is infected. Many people doesn't use anti-virus and neglect the fact that malware can do more than just change around a few words in a word document. Imagine if you work at a company, bring home your laptop to your infected network and then bring back the infected laptop to the company. Chances are they'll notice the infection before something happens, but what if they don't – having someone that can remotely control a computer in your company network is bad news.

In our work we have learned more about malware and how it affects computers, how to protect yourself against it, how to remove it from a computer and what happens if your computer gets infected.

In our work we have also described what malware is, given examples of different kinds of viruses, worms, trojan horses, spyware and adware and how to protect yourself and what to do if you got infected.

Lastly we downloaded different anti-virus software and tested how well they worked when we downloaded a test virus called EICAR, especially used for these types of projects, in different formats.

We noticed that there is a big difference in file size between the different anti-virus programs, ranging from 21.8 MB to 325 MB, so it is important that you select a program that doesn't take up too much space if you don't have very much hard-disk space. The idle CPU-usage is very close to each other in all the programs we tested. The idle RAM usage varies a little bit more, and the active CPU usage is very varied, which means they affect the performance in different ways. Lastly, performance-wise, the active RAM usage was quite varied. Active RAM and idle RAM was very closely related, which means the RAM was not affected by scanning the system. Since a program like Avast Free Antivirus took 35% of the CPU performance while scanning in our test computer, it's important to make sure that you choose an anti-virus program that your system can handle.

Test-wise, Microsoft Security Essentials could remove every threat we tested, regardless of file type, as could Avast Free Antivirus. AVG had a bit more problems, but once you opened the .zip and double .zip files, the virus was detected. Panda cloud could not remove viruses that were detected in .zip and double .zip files. This means that it's important to make the right choice when you select your anti-virus program, as some programs does not work very well, such as panda-cloud.

5 References

[1] http://www.howstuffworks.com/virus.htm 2012-11-12

[2] http://oit.ncsu.edu/resnet/spyware 2012-11-12

[3] http://www.sans.org/reading_room/whitepapers/malicious/code-red-worm_45 2012-11-12

[4] http://www.caida.org/research/security/code-red/coderedv2_analysis.xml 2012-11-12

[5] https://kc.mcafee.com/corporate/index?page=content&id=KB59742 2013-09-02

[6] http://www.f-secure.com/v-descs/eicar.shtml 2013-09-02

[7] http://searchsecurity.techtarget.com/definition/virus 2012-11-28

[8] http://searchsecurity.techtarget.com/definition/virus-hoax 2012-11-28

[9] http://www.virusbtn.com/resources/glossary/file_infector_virus.xml 2012-11-28

[10] http://www.bc.edu/content/bc/offices/help/security/virus/macrovirus.html 2012-11-28

[11] http://surfthenetsafely.com/surfsafely1.htm 2012-11-29

[12] http://antivirus.about.com/cs/allabout/a/whatisworm.htm 2012-11-29

[13] http://lyle.smu.edu/~tchen/papers/network-worms.pdf 2012-11-29

[14] http://www.ehow.com/about_5110319_kinds-trojan-horse-viruses.html 2012-11-29

[15] http://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan 2012-11-29

[16] http://searchsecurity.techtarget.com/definition/Zeus-Trojan-Zbot 2012-11-30

[17] http://whatis.techtarget.com/reference/What-is-spyware 2012-11-30

[18] http://www.ehow.com/list_6457947_different-types-spyware.html 2012-11-30

[19] http://www.spamlaws.com/what-is-a-tibs-dialer.html 2012-11-30

[20] http://antivirus.about.com/od/spywareandadware/a/adware.htm 2012-12-02

[21] http://www.spamlaws.com/what-is-adware.html 2012-12-02

HALMSTAD UNIVERSITY • PO Box 823 • SE-301 18 Halmstad, Sweden • www.hh.se