AIRLINE BUSINESS MANAGER AND HIS/HER ACTIVE PROTECTION AGAINST INFILTRATION

Viktor Šafranko – Miroslav Štancl

Diploma thesis focuses on the antivirus program selection. Before choosing from a variety of market offered antivirus programs, one should know when and how they act and what they can offer. Various infiltrations, which differ in the way in which they can harm the computer, will be discussed, so as their subsequent detection and methods for treatment and removal from the system. After getting a general overview, the thesis will focus on the n the correct antivirus program selection, using Benchmark tests that are performed in independent laboratories for their greater credibility and objectivity. In this paper, three antivirus programs belonging to the 2013 leading antivirus software, were analyzed, namely Kapersky, Norton and Bitdefender. Their different functions in the fight against infiltrations, their maneuverability, table setting and the ability to remove very specific infiltration were compared. Also, the program update and its availability on the Internet cannot be forgotten.

K e y w o r d s: Infiltration, Antivirus program, Virus, Benchmark, Protection.

1 Antivirus Protection Development

Computer viruses endanger computers similarly as real world's viruses endanger men. First documented computer virus was born in 1983. It was created for study purposes and demonstrated during a security seminar. In 1986, first computer virus named Brain was created by Pakistanian brothers Amjad a Basit. Originally, building an antivirus program was not complicated. At the end of the 80s and on the beginning of 90s, lot of users was building antivirus programs for certain forms of computer viruses.

For an expert, to find the boot sector virus was not complicated. However, to write a program that would do that automatically was not so easy. Antivirus programs represent the most common way of protection and defense against viruses. At present, the development of anti-virus programs and security software is considered to be a form of art and enables a man to become a true master of it. [1]

2 Possibilities of Infiltration Attacks

Computer infiltration means unauthorized entering program code into computer system. The term virus has become most common for people, so several types of infiltrations were named by it. They constitute a large group of programs that cause problems to users. Generally, there are many infiltration types, but they have one think in common; they were created in order to perform undesired (often concealed) activities. Infiltrations can be divided into four categories.

.

2.1 Single Action Infiltrations

This type of infiltration is intended for only one action on one computer. They have not the ability to create copies. Among single action infiltrations belong:

Bombs programs intended for disposal of data, files, and programs on the selected site. They are also capable of self-destruction in order to efface. They present a certain way of revenge, terror and also belong to the so-called offensive means.

Troll Infiltrations programs that are created by one of the computer users, designed to entertain their creator and frighten or startle other users. Troll can manifest itself by locking the keypad or typing the swear word. Program itself does not cause damage.

Spy Malwares are programs designed to break into the computer, get some information, sent it to their creator and then quietly disappear. A good spy blinds a trail.

2.2 Multiple Use Infiltrations without Replication

Are intended for a single application, but on a larger number of computers. Among multiple use infiltrations without replication belong:

Mines essentially operate on the same principle as the bombs. Unlike bombs, mines software blast is not a criminal act. Mine destroys only the software, which the user is no longer allowed to have. All other programs and databases remain unaffected.

2.3 Multiple Use Infiltrations with Passive Replication

Malware is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. They are designed for multiple uses. Malware includes:

Chameleons are programs that mimic the behavior of other programs. Their mission is to cause harm to the user, the company that created the original program or to bring unfair benefit to the creator of chameleon.

Trojan Horses – programs, which appear to perform a desirable function but instead drop a malicious payload, often including some kind of destruction like deleting files or formatting the hard disk. Most often enter as executable exe file.

Droppers role of this virus is to transfer the virus to the computer so as not to be espied by a scanner. They are in encrypted form and are related to Trojan horses.

Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information

to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.

Adware is any software package which automatically renders advertisements in order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process.

2.4 Replicate Infiltrations

They can make their own copies, so their range is limited by the counteractions of people. Among replicate infiltrations belong:

Worms are the most common programs that attack computer nowadays. They usually spread via internet in the form of the email attachment. These emails are automatically generated by worms and act very inviting and trustworthy, resulting in that the user starts the program and therefore activates the worm. The worm consequently cause some kind of destruction and without user's knowledge generates emails written under his/her name and send them to the email addresses that it finds in the user's address book.

Rabbits/Replicators are programs similar to worms. They wildly multiply, usually on one computer. In a very short time can overload disk and memory. [2]

2.5 Defending Against Virus Attacks

Before making a decision to buy an antivirus program, one should be familiar with a few points, so-called: Ten Commandments of an Antivirus Protection. Nothing ends by buying the best program. Even though, it may not be able to protect the computer unless some basic antivirus protection rules are respected. An example might be the following ten commandments of an antivirus protection.

a) Regular Antivirus Program Update

Every antivirus program with outdated virus database is inappropriate. Every day a new malware may emerge, from which different mutations can be formed. Data files provided by the antivirus program producer include information enabling reliable detection and removal of the most recent viruses.

b) Never Open an Email Attachment that Is Not Expected

Nowadays, many viruses spread via email and are able to be sent to all the contacts stored in the e-mail inbox, and thus cause problems also to the other users. Such virus, after the e-mail is open, may not end only by spreading itself throughout the email contacts of the affected user. Moreover, it may contain other harmful routines that can dispose data of the affected computer.

c) Keep Control of Your Computer and Its Users

In this case, it is better if the computer or electronic device that is designed for one or more users, is protected by a password. Thus, there would be no unauthorized usage of the computer, which may cause virus attack by visiting the websites or opening the wrong e-mails.

d) Install All Patches In Time

Worms and other scourges like to exploit security holes in the software, namely Windows and other Microsoft programs. If such flaw is detected, producer issues many critical updates (patches) to fix these flaws. These patches are usually available for download on the software producer's website. This rule is applicable mainly to the operating system.

e) Always Check Floppy Disks and CD Media Before Using It

According to the available data, 85% of the recorded incoming virus attacks spread through e-mail, but the traditional ways of spreading malicious code can not be underestimated.

f) Be Cautious About Each New File

This is rule applicable not only for pirate software. There was also a case, when the installation CD from a popular printer company contained the virus. It is important to not install software via the web unless one is absolutely sure what it is. Owner of the web page is not essential because also web pages of the reputable company can contain files infected by viruses.

g) Use More Than One Method of Antivirus Protection

For overall safety, it is not sufficient to use only simple antivirus program that examine the file or directory on request. It is important and desirable for antivirus to know and combine several kinds of protection.

Antivirus monitor that checks opening files in the background.

Integrity checker its task is to record the files and directory modification that may indicate virus attack.

Heuristic analysis searches for viruses not on the basis of the typical code sequence, but by their behavior and expressions.

h) Create a Clean Bootable Floppy Disk And Keep It on the Safe Place.

It can happen that that the computer infected by a virus can not run operating system. However, it does not mean that the hard disk data are deleted. In this case, it is suitable to have previously created bootable floppy disk (obviously free of viruses), which also contains the antivirus program. By using this disk, it is possible to run the attacked computer and cure infected files, or to delete them.

i) Regular Backup

While this is not a rule related to the antivirus protection, but its abeyance enables us to minimize possible damages caused by aggressive virus, unreliable hardware, etc.

j) Do Not Panic

The aim of these rules is no to scare the computer user. Essentially, computer viruses are just ordinary programs. The only difference that makes them dangerous is that they operate beyond the user's control. [3]

3 Active Protection Technologies and Techniques

A vast number of emerging viruses forces us to use antivirus protection as a matter of cause. Nowadays, it is it is quite rare to find a computer without defense. For example, information leak or important data loss can lead to large losses for the airport from economical, as well as the safety perspective.

Experience and expertise are factors affecting the proper functioning of the antivirus software. Rising quality and malware complexity leads to the creation of more complex antivirus programs. Greater spread of the Internet and computer networks results also in the increased amount of malware. This may include an e-mail worm that was not known several years ago. Therefore, by the emergence of new threats is virus protection improving.

3.1 Antivirus System

In the present, it is the most common form of the antivirus programs. It consists of parts monitoring all the essentials input/output points, by which a possible infiltration could break into the computer system. These input/output points may include an electronic mail (email-borne worms) websites (malicious scripts, uploading of infected files), media (CDs, diskettes). Direct internet actualization is part of today's antivirus software update. It presents the complex antivirus solution. This includes antivirus programs such as: avast!, AVG, Norton Antivirus, Bitdefender, Kaspersky Antivirus, NOD32, McAfree Viruscan.

3.2 Antivirus System Update

Antivirus companies are trying to reach the highest quality detection in the time between the discovery of a new infiltration and the release of appropriate updates for antivirus system. Basically, it happens at the time when there is a new threat called "hole" detected by antivirus scanner. If a global problem appears, companies are able to respond quickly and release the update in a similar time. More important is how often an antivirus system is updated on the user side - of course, the more often an antivirus system is updated, the better.

If the user wants to have effective action update, it is necessary to ensure:

- quick response of the antivirus company
- right part setting, downloading updates on the user's side.

Modern antivirus systems try to focus on the detection of previously unknown infiltration. It seeks to fill an already mentioned "hole" by detection methods, including heuristic analysis and generic detection.

Heuristic analysis is based on the ability of antivirus´ program code understanding and reasonable evaluation of acquired information. Generic detection is based on the fact that many new infiltrations are older viruses modifications. This means that for some of the techniques the same or slightly modified program code is used.

Slow internet connection owners are certainly interested in the speed needed for the downloading of update server to the computer. Antivirus companies try to ensure the quickest possible process of the update download, which is affected by the size of update. Method, by which the update size can be reduced, is its division into two independent parts:

- update of the program part of antivirus system. Update fixes flaws in the program section, or expands this section with new features.
- virus database update. It provides us with the new viruses' detection and also modifies the detection of the others.

Antivirus database and its update depend on the particular program. It can be divided into two sections:

complete update – the whole virus database is downloaded again. This update is time-consuming, with an increasing number of viruses. The size of these updates can be determined on MB. Antivirus companies are trying to avoid this kind of update.

incremental update – downloads only those parts of the virus database, which were added to the producer's server since the last update. Advantage is that they download only information which did not occur in the destination yet, and also files already contained in the system are not downloaded again. The speed and size of the update are positive (only a few KB).

3.3 Actions after Identification

Antivirus system is able to apply a large number of activities, which are defined by the user, or selected after the malicious code identification. Deletion of the infected file is the best and most reliable choice. However, often happens that with the infected file also certain data that the file contains are deleted. Temporary alternative is the file rename in order not to activate virus by being started again. Whether the malicious code can be eliminated in non-destructive form of treatment it the first thing the user should be interested in. Treatment can be divided into basic groups:

- algorithmic
- heuristic
- special

Algorithmic Curation

When it comes to an application, the user relies on the accuracy of the identified virus, which is

stored in the virus database. On the basis of such information and procedures, the identified virus is selected from the group and restored to its original form. The successful reconstruction occurs only in that case if one knows how the file was infected and in the case it is non-destructive virus. But even that does not ensure trouble-free future operation. Problem may occur in the case of so-called cavity viruses that attack the parts of files that contain no data. This happens when an antivirus cut out a virus and in its place a different code has to be inserted. Thanks to that fact, the cured file does not have to be set exactly at those places. If the file has internal self-control, it can happen that it will inform about the difference or refuses to cooperate. Macro viruses represent a separate chapter. Format of the document (MS Word) or workbook (MS Excel) is known, so the antivirus has no problem to define the area where exactly a macro virus is situated. If the antivirus system cannot distinguish which macros are harmful or belong to a document, in extreme cases all macros can be removed without major damage. A special chapter belongs to Trojan horses, backdoors. They are cured the infected files deletion, because the Trojan and backdoor files do not contain any other data.

Heuristic Curation

The virus after its launch tries to forward control to the original program. As far as activities are kept under review from the beginning up to this point of the control forwarding, it is possible to remove this section and thereby restore the file to its original form. [2]

File Healing

At some time, some antivirus systems (CPAV) were equipped with the possibility of file healing. Not yet infected file was was prolonged by short control antivirus program. If edited file happen to be infected after its launch, the user was alerted and its treatment was offered. If the control program stored information about healthy file variant, there was no problem to remove the virus file and put it in its original form from the inside. Sometimes these control programs could cause false alarms during the heuristic analysis.

Integrity Control

Viruses can be successfully removed on the basis of information that is automatically saved by the integrity check. If sufficient information on the original file is stored before it is infected, the infected file can be successfully reconstructed to its uninfected form.

3.3 Concrete Antivirus Companies and Their Functions

Antivirus program is computer software that is used for the identification, removal and elimination of computer viruses and other malicious files. Success depends on the capabilities of an antivirus program and recency of an antivirus database. Up to date virus database can be downloaded from the Internet. Antivirus programs can be divided into:

A Definite Purpose Antivirus – programs that focus on detection, and also on disinfection of the particular virus. This is not a full-valued antivirus protection. It is used mainly when a user knows his or her computer was attacked by a particular virus. Unlike a full-valued antivirus system, a definite purpose antivirus offers a more thorough disinfection and greater speed.

A Definite Purpose Antivirus Package – is comparable to the previous antivirus. The only difference is that this kind of antivirus can find and remove a greater amount of occurring viruses.

On-demand Scanner – is of use when a computer is being disinfected. On-demand scanner includes also internet online scanners. Usually, these are different applets, which when connected to a web browser, can scan user´s hard disk. Most of them are operating system freeware.

Antivirus Systems – the most common form of antivirus programs. It monitors all the most important entry points, which would be a possible threat to a computer system: e-mail, web, media (floppy, CD, DVD, Flash ...). The update is via the internet.

In the diploma thesis, following antivirus programs were chosen:

Bidefender Antivirus
Kaspersky Antivirus
NortonAntivirus [2]

4 Evaluation and Design of Active Protection against Infiltrations for Airline Manager

A lot of antivirus programs are offered and it is not easy to decide for the correct and safe one. Tests of popular and not so popular testing companies assessing the various antivirus programs are published every year. Some more detailed tests consist of 10 or more parts that help user to pick up the most suitable antivirus program for the airline manager.

So-called benchmark tests are most appropriate for comparing the functionality and reliability. Author has chosen a set of objective indicators providing comprehensive and realistic information about the field in which antivirus programs can affect the user's system performance. It is the common functions antivirus software testing. Antivirus programs have been tested in Windows 7. PassMark Software carries out objective performance testing on publicly available antivirus products.

In the following table, all the test results of selected antivirus programs that were chosen for the purposes of this work were summarized. The table consists of three independent tests in order to maintain

objectivity when choosing active protection for airline manager.

Table no.1 Resultant Test of the Selected Antivirus Programs

	Bitdefender Antivirus Plus	Kaspersky Antivirus	Norton Antivirus Plus
Boot Time	41,5 s	34,1 s	33,4 s
Total Security Software Boot Time	9,8 s	9,2 s	8,8 s
Scan Time	35,4 s	30,5 s	20,6 s
Total Security Software Scan Time	13 s	42 s	10 s
System Idle Process Memory Usage	37,3 MB	49,3 MB	15,5 MB
Browse Time	73 s	41,7 s	44 s
Installation Time	364,2 s	158,1 s	64,6 s
Installation Size	1095,7 MB	388 MB	592,2 MB
Network Throughput	16,7 s	12,2 s	13,8 s
PE Scan Time	97 s	36 s	93 s
Installation of Third-party Applications	149,4 s	109,1 s	110,1 s
AV-TEST Malware			
Malware Protection	6,0 b	5,5 b	5,5 b
Malware Correction	5,5 b	5,5 b	5,5 b
Whole PC Usability	5,0 b	5,0 b	5,0 b
TopTenREVIEWS			
Malware Detection	10,0	9,38	7,95
Malware Removal	10,0	8,75	7,50
Malware Management	10,0	10,0	8,75
Malware Detection (Standardized Test Score)	100	92	92
Malware Removal (Standardized Test Score)	98	92	77
Evaluation	10,0	9,33	7,95

Based on the tests result table, author would least advise Norton Antivirus as an active protection against malicious code for airline manager. Overall, this program was placed from all antivirus programs on the 3rd place. Such placement is excellent, regarding an amount of antivirus programs that are on the market.

Norton antivirus program with its new SONAR technology, which controls the suspicious activities occurrence in the computer, detects and removes unknown hazards. Norton Management technology is worth mentioning. It is cloud's technology that enables repairing, upgrading and renewing Norton 360 on different computers via the Internet. The installation program size is 592.2 MB, which is the medium value in the performed test and has a very good installation time - 64.6 s. Mentioned antivirus program is on very good level of the site design and is easy to be read. It has lots of interesting settings if there is more than one computer user. Norton website is very well done. User can learn all the antivirus program details in Slovak or Czech language.

The disadvantage of this program is weaker PC protection from malware, Trojan horses and other types of viruses, with a significant loss compared to programs such as BitDefender and Kaspersky. Norton maintained the same position when it came to the Windovs XP, 8 and Vista. It also showed in the TopTenRevievs test, where Norton finished as number 5. It maintained the same position in removing malware from the computer. Anyway, the antivirus program maintained good market position, but in author’s evaluation of the fight against malware was proven incomplete. That is why Norton ranks third. The price of provided product was slightly surprising.

Second place was given to the Kaspersky antivirus, appreciated for its technologies. Phishing

protection was improved, so no one can get to the personal information and antivirus database optimization was also improved. Automatic prevention of diversion or restriction on battery power is novelty. Compared to Norton, its installation size is 388 MB. Regarding antiviral malware defense, it is several times greater than that of Norton and even in detecting and removing malware from the computer. Kaspersky Antivirus protects its users against a broad spectrum of threats, as already mentioned malware, spyware, adware, rootkits, bootkits, and also protects users against identity loss caused by keylogers. It also prevents illegal methods of taking control of the computer.

On the basis of the AV-TEST, Kaspersky antivirus gained the same point number as Norton. The difference occurred in applying the TopTenREVIEWS test, where Kaspersky had its values closer to the Bitdefender antivirus. It is suitable for all types of the Windows operating systems, such as Windows 7, 8, Vista and XP. Author of the thesis liked its web page, which can be read also in the Slovak or Czech language. One can find all the important information on the functionality and installation method of Kaspersky antivirus program. Its interface is very well developed and therefore also for beginners there will be no problem to install and use this program. As for the negative antivirus features, nothing serious was found.

Antivirus program chosen by the work's author as the best one for an active infiltration protection was Bitdefender antivirus 2013. It has excellent anti-virus test results, e.g. effective phishing protection or reliable and accurate antispam. Bitdefender Total Security 2013 contains all sorts of security features and also something extra. Independent laboratories provide excellent rating for all its parts. Bitdefender Total Security with an autopilot keeps the user's interaction at a minimum. Before it asks the user about the decision on security, Bitdefender makes the decision itself.

4 Conclusion

Diploma thesis presented its reader by the possibilities of infiltration's computer attacks. In the work, author has given the reasons for the antivirus programs introduction and function for the airline manager. In the final part of the thesis, author focused on a particular antivirus program that he chose after his study review.

Airline manager's computer should have a sufficient protection, therefore, in the final part of the work, author focused on a specific antivirus program. Computer should posses mainly quality updated antivirus, antispyware, firewall a secure web browser. Everyone can choose computer protection on the basis of various criteria, e.g. control, user interface, or free download.

After studying various antivirus programs present on the market and their individual tests author decided for Bitdefender Total Security 2013 to be the best. He was impressed mainly by its functions and a clear dominance over other antivirus programs. Antivirus protects the computer against threats like spyware, adware, various forms of malware, including worms, trojans, keyloggers and rootkits. Software contains Bitdefender Anti-Theft, which enables the user to track down and find his or her lost notebook. And superb Bitdefender Autopilot, which makes all the work and security decisions for its users and let them to work on the computer without interrupting or slowing process.

BIBLIOGRAPHY

[1] SZOR, Peter: Počítačové víry : analýza útoku a obrana. Brno : Zoner Press, 2006. 43-55, 420 s. ISBN 80-86815-04-8

[2] HÁK, I. 2005 Moderní počítačové víry [online]. 2005. [cit 2013-02-03]. 9-20, 79-86, 90-93 s. Dostupné na internete:<http://www.cmsps.cz/~marlib/bezpecnost/viry/velka_kniha_o_virech.pdf>

[3] Deset pravidel pro účinnou antivirovou ochranu. [cit 2013-02-20]. Dostupné na internete: <http://www.lf1.cuni.cz/deset-pravidel-pro-ucinnou-antivirovou-ochranu>

AUTHORS´ ADDRESSES

Šafranko Viktor, Bc.
Department of aerodynamics and simulations
Faculty of Aeronautics
Technical University in Košice
Rampová 7, 041 21 Kosice
e-mail: viktorsafranko@gmail.com

Štancl Miroslav, Ing.
Department of aerodynamics and simulations
Faculty of Aeronautics
Technical University in Košice
Rampová 7, 041 21 Kosice
e-mail: miroslav.stancl@tuke.sk