ANTIVIRUS SYSTEM AND ANTIVIRUS PROTECTION TECHNIQUES COMPUTER AVIATION BUSINESS MANAGER

Michal Dluhoš – Miroslav Štancl

The theme of the article is about the antivirus system and the antivirus protection of the computer of the aviation company manager and its techniques. The article deals with the techniques of computer antivirus protection manager airline, disinfection storage, antivirus defense methods and possibilities of detection of viral code. Another section is devoted to analysis and description of a selected anti-virus systems. Details the selected anti-virus programs. Conclusion The article is devoted to the choice of the best antivirus for the aviation company manager.

K e y w o r d s : Antivirus, Pc protection

1 INTRODUCTION

Currently, computer security still subject of extensive debates. A few years ago, it was a widely supported view that commons sense is the best data protection installing antivirus is unnecessarily detracting from the performance of your computer.

As it is the world's most dynamic information technology sector of human activity, there is certainly a need for more emphasis. Computer security is considered to be the fastest changing and growing area. Malicious programs can be modified according to their activities soon in several forms, such as spyware, virus, spam or rootkit.

Today's standard PC power manager is entirely different from the level as it was few years ago. An antivirus program is not developed only from the aspect of security, but also in terms of compatibility. Today's antivirus programs contain a number of modules and they are no longer mere web-shields.

2 VIRUS PROTECTION TECHNOLOGY

2.1 Disinfection of memory and its scanning

Virus authors are well aware of the fact that the virus replicates itself faster when active in memory and captures while calling the operating system. The early viruses like Brain, or Jerusalem, always remain resident in the memory. Scanning memory in DOS was relatively an easy task. Because DOS uses Intel processors operating in real mode, it was not possible to make more than 1 megabyte of physical memory. Memory scan is a must for all operating systems. Once the virus starts and becomesd active in the main memory, it can use different techniques and hide from the searching devices.

2.3 Scanning memory in kernel mode

Scan memory in kernel mode is essentially a very similar implementation in user mode. In kernel mode, however, will always secure scanning. In addition, the scanner search for viruses in the upper 2 gigabytes of space adresovacieho core. Currently, the systems used in only a few viruses that run in kernel mode.

2.3 Disinfection of memory

Memory scanner should work closely with on-access scanner and should recognize the same set of viruses known antivirus products and components. On-access scanner should detect most known viruses, although in some processes active virus code. But can not prevent the virus infects other objects, because the virus can be objects that have been cleaned, re-infect. Typical antivirus software can detect the virus in the applications before them is to code the virus entered. Viruses can become active in the following typical situations:

- Virus scanner was not installed on your computer.
- This is a new virus scanner and must be updated to detect it.

2.4 Termination of a process that contains the virus code

Probably the easiest way to disable the virus in memory, the entire job is complete, in which the virus was detected memory code

scanner. This can easily be done using API TerminateProcessQ. Active virus code is usually attached to an application user can be infected if an ordinary end user process lost important data. The application may also have several open database files, so in the event of termination of the process was not possible to maintain their consistency. For these reasons, TerminateProcess should be used in cases where the code of the virus is active in a separate process, for example, viruses WNT / or REMEX W32/Parvo.

2.5 First generation scanners

Typically, virus detection described in quite simple level. Anti-virus scanners are described as a simple program that searches the sequence of bytes extracted from computer virus contained in a file or memory. This is truly one of the most popular methods for detecting computer viruses. The current anti-virus software is used to detect complex viruses much more interesting techniques that first-generation scanners can not do.

2.6 Second generation scanners

Second-generation scanners used a precise identification of which helps to improve the detection of computer viruses and other malicious programs. Detection of the structure was developed by Eugene Kaspersky, and is especially useful in the detection of macro viruses families. Instead of removing the single chain or a checksum scanner sets of macros macros rather processed line by line and release all the unimportant commands. The result is the body of the macro structure, which contains only the necessary malicious code, which normally occurs in macro viruses.

2.7 Personal laboratory for analysis of virus

One of the most overriding requirements for analysis of malicious code installation system dedicated just for this purpose. The codes for replicating virus should not be used for other purposes and need to be always totally cleaned thoroughly, preferably after each test.

Malicious code can be identified using the following techniques:

- Monitoring changes in executable files.
- Analysis based on goat files.
- Monitoring changes in the registry.
- Monitor processes and threads.
- Monitoring of network ports.
- Track and capture traffic on the network.
- Trace system calls.
- Debugging.
- Emulation code.

3 DESCRIPTION AND ANALYSIS OF SELECTED ANTIVIRUS SYSTEMS

An antivirus program monitors all the most important entry and exit points, which the virus could penetrate into the computer system. Antivirus data by revealing dangerous virus database, which contains templates of various dangerous files.

3.1 AVG AntiVirus 2011

AVG Antivirus 2011 is a complete security package that offers protection in addition to basic and advanced. The starting point for users of AVG Antivirus 2011 is the main center, which serves to manage all components of the package and extends the default Windows security center.

Fig. 1 – AVG Dashboard display

Resident Shield active checks for new files to your PC for potential threats while online scan monitors transmissions over any network connection, and instant messaging services. Anti-Rootkit component is automatically installed into your web browser and a search engine then judge each site on the list prior to visiting. Special protects users from phishing separate components Identity Protection. LinkScanner examines web pages and search engine requirements for malicious content, and warns the user when you

move to places that might contain an active threat. The software includes antivirus and antispyware protection as well as complete protection against malicious online webm and downloads. AVG protects against hackers, adware and malware that come through e-mail. AVG checks and outgoing e-mails. Of course, the program protects against other forms of malware, including worms, keyloggers, Trojans and rootkits. AVG strength comes from multiple layers of protection and advanced technologies. The core of the antivirus module is supported by a proactive heuristic detection and protection AVGProtection Network. In combination with proactive analysis and realtime protection Cloud Antivirus is AVG Anti-Virus comprehensive and effective program.

Unlike its competitors, who offer assistance through the visible buttons on their panels, AVG gives orders for local and online support in the Help menu. AVG is one of the smallest sites of support among the competition.

3.2 Kaspersky AntiVirus 2012

Kaspersky Anti-Virus is one of popular antivirus programs not only for household use, but also to protect corporate networks and servers. Promotes quality control of e-mails in a number of clients, anti-spyware, check visited web sites and continuous identity protection.

Screen user interface is divided into the protect PC, which displays the current status of computer security, and sliding the toolbar, which allows access to the full feature set Kaspersky.

Fig. 2 - Kaspersky AntiVirus 2012 Dashboard

The most significant improvement if the Kaspersky Anti-Virus 2012 is a cloud-based protection. A new user interface in terms of the Virtual Keyboard. Kaspersky 2012 is further implemented in a web browser. Users of ther Internet Explorer, Firefox and Google Chrome will see two new buttons on their toolbar. Virtual Keyboard for one and one for Kaspersky URL Advisor, which warns the user before accessing the malicious Web site.

Kaspersky is designed to protect PCs from several aspects, the effective detection, prevention and elimination of all forms of malware. Antivirus software is equipped to protect from traditional viruses, but also advanced protection technologies against new and unknown threats. In addition, several tools and web-specific features that are usually found only in complex Internet Security Suites to detect worms, rootkits and Trojans. The Watcher, monitors and records the activity of applications and their behavior. But more than just detect stealth hrozbieb, System Watcher can remove any malware that was created or distributed in this process. Support in the control panel is composed of:
online troubleshooter, a database of frequently asked questions, auxiliary active forums with technical support.

3.3 NOD32 AntiVirus 5

Very user-friendly antivirus that has stood the test of Virus Bulletin recognized several times in a row. With Threat Sense technology detects even unknown threats that other antivirus programs do not recognize.

ESET AntiVirus 5 used to simplify the task drop-down menu, which features are popular and last used commands.

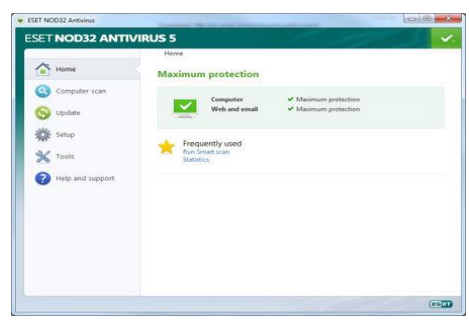

Fig. 3 - NOD32 AntiVirus 5 Dashboard

The new Gamer Mode feature. Gamer Mode suspends disk and memory-intensive applications where the user is watching a video or

computer game playing. Live Grid uses information from millions of users worldwide to identify potentially dangerous files and applications. Finally AntiVirus 5 introduces a new heuristic detection technology system host-based Intrusion Prevention System (HIPS), which detects and blocks the active application of suspicious activity. NOD32 supports scanning local drive, network drive or removable media.

Eset NOD32 is equipped with all essential features and technology to the airline manager's computer is protected against traditional threats such as viruses, worms, Trojan horses, spyware and rootkit. It is also fully armed with the full protection of your PC when online manager. Eset is working behind the scenes with protection against dialers, adware and software, recording keystrokes. Eset NOD32 integrates protection to e-mail from viruses and other malware. Threat Sense has now more than 20 new features that enhance its performance in the diagnosis, their use and detection of malware. ESET NOD32 Antivirus is password protected to prevent foreign uninstall.

ESET expands your knowledge base and the possibility of posting video tutorials. The user can request assistance through social networks like Facebook, Twitter and YouTube.

4. SELECTION OF THE BEST ANTIVIRUS FOR PC OF THE AIRCRAFT COMPANY′S MANAGER

As with all consumer products, antivirus programs are good, bad and average. Virus protection options are varied. In the article we evaluated the best antivirus on the achieved results in the following areas: scope, efficiency, easy installation and setup, easy use, features, updates, and support.

4.1 Evaluation of the proposal and virus protection

Table no. 1 summarizes all the information about the selected antivirus that could be a good choice for protecting your computer manager airline. The table includes a criterion relating to the support, transparency, manageability, updates and antivirus features selected.

	NOD32 5.0	Kaspersky 2012	AVG 2011
Memory Use	66,3 MB	23 MB	29,6 MB
Reboot time	5,9 s	16,5 s	24,9 s
Installation Size	309 MB	551,1 MB	481,6 MB
Initial Scan Speed	44,3 MB/s	34,4 MB/s	32,4 MB/s
Subsequent Scan Speed	262,6 MB/s	284,4 MB/s	209 MB/s
Subsequent Application Launch Time	0,068 s	0,156 s	0,149 s
Antivirus Protection	96,8 %	76,2 %	64 %
Other	+ + +	+ +	+

Table 1 - Evaluation of the data

The resulting real basis of Table. 1 is a manager for an airline at least suitable AVG Antivirus 2011th The program includes AVG LinkScanner, which provides protection against ever-increasing number of Internet threats. AVG LinkScanner technology examines the content of websites and makes sure they are secure sites. The AVG protects your computer against hackers, adware and malware. The program finds malware, including worms, keyloggers, trojans and rootkits. AVG tests alone can get the computer, but takes acceptable 29.6 megabytes of RAM. Worst hit in program evaluation and scanning speed of the first in the current scan. The first scan is the average speed achieved only 32.4 megabytes / s in normal scan is only 209 megabytes / sec. The disadvantage of this program is to extend the closing of a computer with a 24.9. The main drawback is the poor protection of PCs against malware, adware, worms, Trojans and other types of viruses. The international company AV Comparatives got AVG Antivirus 2011 two of the three rating stars, which is a weak average. Also, AVG Antivirus 2011 does not excel at either their removal. The assessment was given at least AVG stars through a small technical support and heavy uninstall a program from your computer.

Central choice for manager would be Kaspersky Antivirus 2012th. It focuses on the most anti-viru protection but also promotes protection against spyware and other malicious code. AV Comparatives, which performs virus and malware tests Kaspersky rated 3 out of 3 stars. AV-Test for testing in June 2011, Kaspersky rated 16 points out of 18 on Windows XP. In the second set of tests that took place on Windows 7 in March 2011, Kaspersky got 14 out of 18 points. Kaspersky includes quality control of e-mails and web sites with continuous protection of your identity. Kašperk 2012 uses the least memory (only 23 MB) but the installation dimensions of 551.1 megabytes are the largest among the selected programs. The little lag when running applications that extend about 0.156 s. Kaspersky got 2 stars for on-line support and transparency features.

The best test is NOD32 Antivirus 5.0. The latest generation of ESET NOD32 Antivirus protects most airline computer manager from threats such as worms, malware, adware, spyware, Trojans, keyloggers and rootkits. AV Comparatives rated in the August test, NOD32 highest mark with 3 stars in the On Demand test. While Proactive test in May 2011, only reached the average rating for supernumerary false alarms. AV-Test runs a test every few months for various Windows operating systems. In a test in August 2011, ESET got 11 out of 18 points for Windows 7 platform. The June test was 13 out of 18 points in Windows XP and the score of 12.5 out of 18 on Windows 7 in March. The Virus Bulletin 100% mark achieved. NOD32 passed the VB100 test in 2011 as the best of 52 tested systems from April 2002. NOD does not burden the system and quickly find possible threats. Although the program takes up 66.3 megabytes of memory but only reboot extend time of 5.9 s. It also achieved the best time to start time extension application. Running extended only about 0.068 s. The evaluation reached 3 stars for overall impression, clarity and excellent anti-virus protection. The disadvantage is the contact with customer support through off-line forms.

5 CONCLUSION

Internet in recent years, expanding at high speed. It is not only a source of information but also means of communication. Service pack installation is the first step towards the protection of operating system. It contains a range of improvements and primarily system security. Another important step is to install a high-quality antivirus software and a reliable firewall. The antivirus program is to prevent infiltration of unwanted files into your computer, using many methods that have been developed for years becoming highly refined. For example, real-time protection guards all run programs and opened documents. Firewall allows filtering and traffic monitoring data packets on the network. Each computer is connected to the Internet to send and receive large amounts of data. Firewall provides an overview of applications involved in network traffic and tells you which ones just receive or transmit data. Like the firewall and the antivirus software, should now be on every PC. Some antivirus systems contain all the security in one package.

Based on reviewing the data, literature and tests the best computer security program manager for the airline is NOD32 Antivirus fifth This comprehensive package of services to find and remove computer viruses, Trojan horses, worms and other types of threats. Using ThreatSense technology detects even unknown threats that other antivirus programs do not recognize. It does not burden the system and protects the slower computers.

Installing antivirus and firewall is not the end of computer protection. In my experience, it is appropriate to waive the integrated web browser Internet Explorer and install the Opera browser for example. It is not a very good approach to visit sites with illegal and questionable contents. It is here, where malware is everywhere, in fact. Most frequently in the form of codes hidden in the pages or in pop-ups and false Internet addresses.

Computer Security is an important step for the smooth working if a manager also protecting your computer from data losses. Protect ion against malicious code needs not only well built and maintained anti-virus protection, but also

consistent patching holes in operating systems and applications, as well as training of users.

BIBLIOGRAPHY

[1] SZOR, Peter: Počítačové viry : analýza útoku a obrana. Brno : Zoner Press, 2006. 429-464 s. ISBN 80-86815-04-8
[2] MRNUŠTÍK, Jiří : VirusScan. : Antivirový program nové generace. Praha : Grada Publishing, 1994. 10-50 s. ISBN 80-71691-58-5
[3] KOCMAN, Rostislav : Jak se bránit virům, spamu, dialerům a spyware. Brno : CP Books, 2005. 92-128 s. ISBN 80-25107-93-0
[4] SZOR, P. 2006 Techniky antivirové obrany [online]. 2006. [cit 2012-02-11]. Dostupné na internete: <http://www.zonerpress.cz/download/pocitacove-viry-analyza-utoku-kapitola11.zip>.
[5] SZOR, Peter: Počítačové viry : analýza útoku a obrana. Brno : Zoner Press, 2006. 525-568 s. ISBN 80-86815-04-8
[6] ALLEN, J. 2010 Review of AVG AntiVirus 2011 [online]. 2010. [cit 2011-11-22]. Dostupné na internete: <http://www.antivirusware.com/avg/antivirus/>.
[7] TopTenREVIEWS 2011 Kaspersky Anti-Virus 2012 [online]. 2011. [cit 2012-02-13]. Dostupné na internete: <http://anti-virus-software-review.toptenreviews.com/kaspersky-review.html>.
[8] ECHES 2011 Eset Nod32 Antivirus 5 [online]. 2011. [cit 2012-03-05]. Dostupné na internete: <http://eches.net/download-eset-nod32-antivirus-5-review/>.
[9] Toptenreviews.com 2012 Best AntiVirus Software Review [online]. 2012. [cit 2012-02-11]. Dostupné na internete: <http://anti-virus-software-review.toptenreviews.com/>.
[10] AntiVirus Performance Tests [cit 2012-03-20]. Dostupné na internete: <http://www.antivirusware.com/testing/performance/>.

AUTHOR´S ADDRESS

Michal Dluhoš, Bc.
Košice, Slovenská republika
e-mail: michal.dluhos87@gmail.com