Bulletin of the *Transilvania* University of Braşov • Vol. 8 (57) No. 1 - 2015
Series I: Engineering Sciences

PRESENTATION OF OUTSTANDING SOFTWARE SOLUTIONS AVAILABLE FOR COMPUTER PROTECTION AGAINST SECURITY THREATS ON THE INTERNET

Constantin Adrian MANEA[1]

Abstract: *The protection of personal computers and corporate systems against more and more ingenious, more sophisticated and harmful security threats is an integrated complex of activities to be carried out continuously and with increased intensity, with the help of specialized protection programs, the steps to follow rigorously and cyclically being: prevention, detection, removal, recovery, prevention... Starting from the issues to be pursued in choosing a powerful antivirus (the malware detection rate published on the Internet, the scanning speed, the resources used by the system in order to operate and the technical support provided) we will highlight in the material the advantages/benefits of using the Bitdefender Kaspersky solutions, security applications evaluated and rated to be the best on the market in recent years.*

Key words: *information system, vulnerability, security, antivirus, Internet.*

1. Introduction

The statistical data provided by the National Center for Cyber Security Incident Response - CERT-RO [3] for the years 2013 and 2014 confirms that the cyber threats on the national cyberspace continue to diversify, are on the increase, and most alerts received refer to systems infected with various malware variants.

CERT-RO draws the attention that the devices or network equipment used at home (wireless routers) or those that are part of the Internet of Things category (IoT), such as web cameras, smart TVs, Smartphones or printers, once connected to the Internet, become the target of hackers due to the lack of protection and their vulnerabilities are exploited by the attackers in order to gain access in the network in which they are used or in order to launch attacks on other targets in the Internet network accessed.

Statistically speaking, the evolution of the increase in cyber security alerts in Romania in 2014 with 81.4% compared to 2013 as well as the 9.1% increase in the number of unique IPs involved in at least one cyber security alert in the same reference period confirms that Romania today cannot be considered just a country generating cyber security incidents, for entities in Romania were and are the target of foreign and complex targeted attacks, of the type APTs (Advanced Persistent Threats). The data analysis above demonstrates the intermediate/ transit character of some connected

[1] Dept. of Automation and Information Technology, *Transilvania* University of Braşov.

information systems whose security was affected, systems that are part of the national cyberspace.

These negative results regarding the cyber security confirm that security threats are increasingly sophisticated and harmful to users, while the authors of spy software create malicious programs, sometimes difficult to remove, which can undergo continuous "mutations" and spread on the Internet in minutes. At the same time, information threats appear in more and more combinations, with multiple and/or disguised forms, being able to attack simultaneously computer systems on several levels.

Defined as events occurring in the network with implications on the security of a computer or the network itself, the cyber security incidents affect the security and integrity of networks and services. And yet we can not speak of a uniform definition, common to all cyber security incidents, the term sometimes being equated with the notions of breach, malicious attacks or Advanced Persistent Threats (APTs) [5].

Facing the IT security threats, the first reaction of any user of an electronic communications network must be to provide a minimum security by installing a latest generation antivirus and antispyware or through firewall hardware or software.

The existence of an antivirus program is absolutely necessary in an operating system, thanks to the increasing number and the diversity of large malware, the role of an antivirus being to detect the presence of infected files and remove them [1].

2. The Analysis of the Evolution of Cyber Security Threats

In 2014, CERT-RO - national contact point on cyber security incidents - has received and processed over 78 million cyber security alerts that have affected more than 2.4 million unique IPs in Romania involved in various types of cyber security incidents [3]. The 2.4 million unique IPs involved in at least one cyber security alert in 2014 represent 24% of all unique IPs allocated in the Romanian cyberspace, this number being on the increase compared to the 16% of unique IPs affected by incidents in 2013.

The same statistical sources confirmed a number of 10,759 domains ".ro" notified by CERT-RO as being impaired during the year 2014, with 5% more domains than during 2013 (10,239 domains) which represents approximately 1.5% of all areas ".ro" registered in Romania in December 2013 [3].

On global level, the statistics on cyber security incidents are on the increase in 2014 compared to 2013. Thus, in 2014 the total number of cyber security incidents detected globally in companies increased by 48% compared to the previous year, reaching 42.8 million global events, as evidenced from an analysis made by PwC - The Global State of Information Security Survey 2015 [4], and the financial losses caused to the organizations by such incidents were estimated to $ 2.7 billion, increasing with 34% compared to 2013.

In Europe, the number of security incidents detected increased by 41% compared to 2013, the number of incidents in North America increased by 11%, while in Asia there was an increase of 5%. South America is the only region in which there was a decline from this point of view, of about 9%, the decrease in the number of notifications being justified by the reduction by 24% of the cyber security budgets in the region and hence of the organizations' financial resources for the implementation of the computer security measures.

The increase in the number of security incidents detected and reported is due to the regulatory framework that imposes an

obligation on reporting security incidents to the providers of public electronic communications networks, but also of the investments made by legal entities, public or private, as well as the individual users to install in their own computer networks antivirus and antispyware programs.

3. Software Protection Solutions

The organization AV-Comparatives.org does every year antivirus software simulations in order to analyze the capacity for real-time protection of the programs offered on the market, publishing reports describing tests for the detection of the malicious files and programs potentially dangerous, performance tests, evaluating the heuristic engine, protection dynamic tests [2] (Table 1).

The conducted final annual rankings propose the following categories in which the antivirus products are divided: Advanced+ (very good protection), Advanced (good protection) and Standard (standard protection).

Software evaluation results Source: AV-Comparatives Table 1

Sofware protection solutions	Real-World Protection Test - 2014 Aug to Nov	Removal Test - 2014 Nov	Performance Test - 2014 Oct	File Detection Test - 2014 Sep	Malware Removal Test - 2014 March to Oct
BitDefender	Advanced +	Advanced +	Advanced +	Advanced +	Advanced +
Kaspersky Lab	Advanced +	Advanced +	Advanced +	Advanced +	Advanced +
ESET	Advanced +	Advanced	Advanced +	Advanced	Advanced
AVIRA	Advanced +	Advanced	Advanced +	Advanced +	Advanced
Panda	Advanced	Advanced +	Standard	Advanced	Advanced +
AVG	Advanced +	Advanced +	Advanced	Standard	Advanced +
McAfee	Standard	Not tested	Standard	Advanced	Not tested

Among the programs offered on the market, we are proposing an analysis of the best two software protection solutions at this moment - BitDefender and Kaspersky Lab, solutions which have proven their reliability over and over in the recent years in terms of the analysis criteria they have been subject to by the organization AV-Comparatives.org. [6]

3.1. Bit Defender Products

Declared after rigorous evaluations of antivirus products on the market by the Austrian test lab AV-Comparatives [2] as the best product of 2014 and surpassing its rival for the second time - Kaspersky Lab, the Romanian product BitDefender, with the current version 2015 is a security solution that provides maximum protection and is easy to install and employ by the users.

Among the improvements brought to the variant BitDefender Antivirus Plus 2015 for individual users, we mention the quick scan function of the vulnerability by using the unique technology Photon, the weekly safety report with the possibility to view the issues addressed since the installation of the program and the taking-over by the autopilot of the optimal security decisions without displaying pop-ups and system alerts that are automatically blocked, without disrupting the applications currently running. These functions are shown in Figure 1.

The Wallet function of the program ensures personal privacy, the safeguarding of passwords and of the login details in social networks.

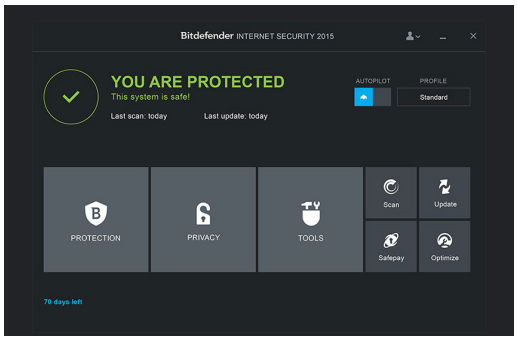

Fig. 1. *Screenshot BitDefender Antivirus Plus 2015*

The antivirus solution for the individual users BitDefender Internet Security 2015 constantly monitors the Internet connections through the bidirectional firewall, which increases the safety of connecting through Wi-Fi. Based entirely on Cloud technology, it diverts unwanted e-mails from the Inbox to Spam.

The downloads from the internet through the BitDefender Tune-Up function decrease in duration, the unnecessary files being removed from the hard disk and thus increasing the computer performance.

The Internet Banking application, by using the secure BitDefender web browser Safepay, protects the online transactions, being fully integrated to the Wallet function. The Parental Control provided by BitDefender is improved, the component being moved in Cloud, can block or restrict the Internet access during certain time intervals, allowing remote monitoring of the children's online activity.

Regarding the BitDefender business solutions, BitDefender Small Office Security (Cloud Console) protects the small companies with up to 250 desktops and servers, without the need for expensive hardware and without affecting the performance of the users' computers, and BitDefender Gravity Zone is the security solution for the medium to large organizations with new, private cloud architecture, running on virtual levels and is designed to enable organizations to secure their IT assets, protecting from hundreds to hundreds of thousands terminals.

3.2. The Kaspersky Lab Products

From the first product offered in 1997, Kaspersky Anti-Virus, the Russian company Kaspersky Lab has developed and provided quality security software products, which shows the level reached today: third in the world as a company that provides software solutions for IT security, with 31 offices in 30 countries, providing software products to over 300 million individual users and to more than 250,000 companies in the world.

Declared by AV-Comparatives [2] *the Product of the Year 2011* - Kaspersky Internet Security 2011, respectively the *2012 product* - Kaspersky Endpoint Security 2012, the software versions offered in 2015, both to the individual users and to companies come with advanced security cloud and anti-phishing technologies.

Kaspersky Antivirus 2015 for individual users provides maximum protection against the latest malware attacks also detects the URLs used by hackers through advanced anti-phishing technologies and prevents the exploitation of system vulnerabilities, scanning, analyzing and neutralizing these vulnerabilities.

Kaspersky Antivirus 2015 is fully compatible with the latest operating systems developed by Microsoft, integrating the latest security solutions: integration with the Windows Security Center functionality or integration with Early Launch Anti-Malware (ELAM) technology, meaning that protection is provided even before the boot.

Well integrated with Windows 8.1 and all its security and network features, Kaspersky Internet Security 2015 automatically disables Windows Firewall

and Windows Defender, thus eliminating any potential conflicts and performance issues. In case of a malware infection, a user who has installed Kaspersky Internet Security will benefit from a thorough but slow verification, compared to the processes used by other security products, as the Kaspersky application will recommend the reboot in order to clean it, then will launch Microsoft Troubleshooting Windows in order to check for system problems that could be caused by the malware activity or the disinfection process.

Kaspersky Internet Security users benefit from a rapid protection against emerging threats employing cloud technologies that use information from the Kaspersky Security Network (KSN) - Kaspersky Lab network monitoring threats, a globally distributed network which gathers permanently information regarding new threats from millions of computers worldwide.

Other tools and features offered by Kaspersky Internet Security - variant 2015 are: *the Anti-Banner module* (with extensions for Internet Explorer and Firefox only) - a module that removes ads from web browsing; *the Virtual Keyboard* - a keyboard on the screen that should be used when the user wants to be sure that the data s/he enters is not registered by other applications or malware, *Privacy Cleaner* - cleans recent orders computer history, accessed files, cookies, cache, logs etc.; *Browser Configuration* - this tool analyzes the configuration of Internet Explorer and recommends improvements to its security settings.

Internet threats on the mobile device or personal computer are the same regardless of the operation performed (banking, various social networks and in e-commerce), for which Kaspersky Internet Security - Multi-Device is the solution with single license which can protect the digital identity, financial data, private information and the children (in the latter case, the application blocks downloads and access to inappropriate content from the web, manages the accessed social networks and prevents children from transmitting essential personal information).

Kaspersky Small Office Security is a product designed for microcompanies, easy to install, set up and use in order to provide integrated security to PCs and servers by administering the security of the entire network from a single point. An advantage offered by this product is real-time protection either by making a backup of the important data of the company, by storing and transferring securely important information in encrypted files and protected by passwords, or by using Password Manager module in order to generate, store and automatically enter strong passwords, difficult to decipher, or by using the File Shredder module to permanently delete confidential information.

4. Conclusions

Given the large number of options for software security, we can conclude that the antivirus applications market is profitable due to the competitivity of products and the need to develop security products for all instruments connected to the Internet, on the one hand, and because of the exponential development of Internet threats (viruses, worms, Trojans, phishing, rootkits) to which the security solutions must respond.

Given the role of an antivirus program to detect the presence of infected files and to remove them, in choosing an antivirus program we should take into account several criteria such as:

1) The detection rate - it is recommended to opt for an antivirus product with a 97% detection (from the analysis performed both protection solutions presented meet this criterion);

2) The speed of response to new threats, the best option being a protection solution that recognizes new threats in a short time;

3) The technical support offered by the developer is another criterion as users can thus resolve their uncertainties regarding the configuration and settings of the program [1];

4) The usage of the user's computer resources is desired to be as reduced as possible so as not to slow down the activity of the system while the antivirus program performs its routine scans and disinfection. For these reasons, the antivirus programs feature special modes type GAME MODE (option used during a game that suspends automatic scans, notifications or the up-dates of the antivirus);

5) The scan speed may weigh considerably when choosing an antivirus protection solution, while the volume of information stored and the complexity of the operations carried out require increasing sizes of the hard disks.

Although classified as Advanced+ in AV-Comparatives ranking produced in March 2015 [6], the products analyzed by us - BitDefender and Kaspersky - are lagging behind other software protection solutions such as ESET, Panda or TrendMicro on the rate of false alarms, the latter protection solutions generating less false alarms for clean files.

Acknowledgements

This paper is supported by the Sectorial Operational Programme Human Resources Development (SOP HRD), ID134378 financed from the European Social Fund and by the Romanian Government.

References

1. Mihai, I.C.: *Securitatea Informaţiilor* (*Information Security*). Craiova. Sitech Press, 2012.
2. AV: *Independent Tests of Anti-virus Software.* http://chart.av-comparatives.org/awards.php?year=2014. Accessed: 15.03.2015.
3. CERT-RO: http://www.cert-ro.eu/articol.php?idarticol=918. Accessed: 28.03.2015.
4. PwC: *Global State of Information Security Survey 2015.* http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml#. Accessed: 20.03.2015.
5. *Cyber Security Incident Response Guide - Version 1:* http://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide.pdf, p. 10-12. Accessed: 30.03.2015.
6. http://www.av-test.org/en/antivirus/home-windows/ Accessed: 28.03.2015.