SINGIDUNUM JOURNAL OF APPLIED SCIENCES
ECONOMICS. MANAGEMENT. TOURISM. INFORMATION TECHNOLOGY. AND LAW

SINGIDUNUM JOURNAL 2012, 9 (2): 14-20
ISSN 2217-8090
UDK 343.983:004.056.53
Original paper/Originalni naučni rad

FORENSIC INVESTIGATION OF "TROJAN DEFENSE" IN VIRTUAL ENVIRONMENT

Gojko Grubor[1,*], Nebojša Ivaniš[1]
[1]Singidunum University, Department for Informatics and Computing
32 Danijelova Street, Belgrade, Serbia

Abstract:
This paper presents an example of a malware attack on a virtual computer. Human factor and social engineering techniques are believed to play a major role in malware attacks. Insufficient education of the user regarding the information safety facilitates further action of the attacker. The attacker writes the malware code if necessary - as a key logger, downloader, etc. Every attack includes good preparation, port scanning, collecting information about antivirus software and target computer usage, considering the scenario of the attack, and choosing the best timing and method of the attack. The paper discusses anti-forensic role of Trojans in a corrupt virtual computer from which the abuse was committed, without the owner's knowledge. Furthermore, the paper provides more information about the experimental verification of forensic activities aimed to prove the so called "*Trojan Defense*" in virtual environments.

Key words:
malwere,
Trojan,
Trojan defense,
cloud computing,
virtual machines.

INTRODUCTION

In this paper we tested the case of forensic analysis of a *zombified* virtual machine (VM). There is hardly any forensic analysis of actual cases of attacks on the VM within the published literature, probably due to the fact that the phenomenon of VM attack has not still become the standard in the world of computer crime (Grubor et al. 2010; Mather et al. 2009). Virtualization of both server and hardware parts represents the basis for modern Cloud Computing (CC) systems (Barrett and Kipper, 2010). The CC system becomes a challenge not only for the new sophisticated types of abuse, but also for digital forensics (DF) (Lillard et al. 2010). It is well known that numerous anti-forensic activities can remove typical forensic clues and leave the computer without any apparent evidence. However, some clues that could be detected by modern forensic tools (Milosavljević and Grubor, 2009), always remain in a VM. The fight of digital forensics (DF) against the attacker's anti forensic activities requires establishing good communication between service providers in order to monitor the system. Also, it is known that most of the malware present on the Internet[1]is written for Microsoft Oss. The centralized system of information protection is necessary in order to enable easier monitoring of resources in the CC. Authentication and access of one computer to another generates a vast amount of information. Intrusion into someone's computer is not easy to perform, but it is not unachievable. A typical attacker uses *Linux* operating system (OS) and specific tools for malicious hacker attacks, out of which mainly Trojans for long-term exploitation. However, the details of preparation for the attack and overtaking of VM's are not the subject of this paper and can be further found and analyzed in the literature (Veinović and Ivaniš, 2011). Once he opens the *backdoor* and takes control of the VM, the attacker has the ability to use the remote desktop access. The DF's task is to look for the evidence and prove or dispute the "Trojan defense" of the owner of the computer, that is, the victim of Trojan attacks (Grubor et al. 2010).

1 The Help Net Security News: About 85 million new sophisticated malware has been generated on Internet in 2011.

* E-mail: ggrubor@singidunum.ac.rs

EXPERIMENTAL VERIFICATION OF "TROJAN DEFENSE" IN VM-I

Figure 1 shows the experimental environment. The physical host is running the VMs which are domain members. The OSs used in the experiment are *Microsoft Windows 7*, *Microsoft Server 2008 R2* and *Linux*. Two physical machines are used with the installed Microsoft and Linux OSs. They are not domain members, and their role is to conduct the attacks. The domain can be accessed via *VPN*[2] channels from the outside. The CA server acts as a *root* certification authority, thus issuing certificates to its subordinate *CA* servers. Afterwards, the two subordinate *CA* servers takeover the roles - *role*. The role of *TMG Fore Front 2010*[3]server is to record the flow of network traffic as well as a *firewall*. There is a test site on the *Web* server which can be accessed over the *HTTPS* security protocol. The *Exchange 2010* server holds the electronic mailboxes for messages. Sending, receiving and controlling the mailbox is possible in two ways: through the *Outlook Web Access*, with direct access to the *Web* site, or through installing the *Outlook* application from the *MS Office* package.

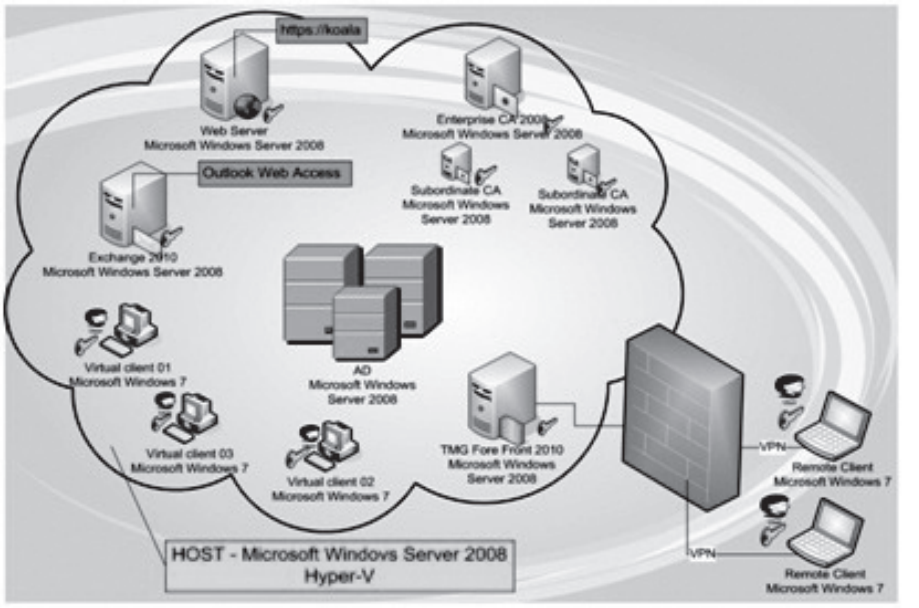

Figure 1. Environment for the experimental verification of anti- forensic activity

2 VPN - virtual private network – protected channel that is used to connect users from remote locations to intranet and local networks.

3 TMG - Forefront Threat Management Gateway 2010 – successor to ISA Server, has the role of a protector of the internal network, as well as monitoring of the entire package flow into and out of the network with analysis capability.

Anatomy and trends of Trojan attacks.

Each malware is written in a specific programming language, and the code adjusts to the attack scenario. The attacker considers which method to use for distributing malware to the user. The most common scenario is deception by social engineering. For instance, in an attack scenario, the attacker makes a copy of a popular *website* where he offers a free branded anti-virus application. Unknowingly, by downloading the application, the user installs *Trojan key logger* or a *downloader* to his computer. Then, using the *root kit* technique that conceals the presence of a Trojan, he can attack by opening the back door. The attacker gets diverse information from the zombified computer, such as user's passwords, recording keystrokes (*keylogger*) or downloading the new malware from the infected web sites (*downloader*). Trojan's program code sends the collected information in a form of an e-mail message or a file to the attacker. DF can use the tracking of the e-mail's path as evidence. With the collected info (username and password), the attacker begins to attack the targeted computer. He escalates privileges to administrator rights. The attack begins by connecting Trojan's server component, installed on the victim's computer, and its client component on the attacker's computer. In the majority of cases, applications for the attack are written for Linux OS. The stolen user's identity (user name and password) is used to access the attacked computer. By running certain services, the attacker takes control of the attacked, now the zombified computer. He performs a variety of illegal actions (spam, DoS and DDoS attacks, extortion of money, etc.) as well as activities the computer owners are unaware of. Many of the B*otnet* networks are based on zombified computers, numbering up to 2.4 million of corrupt computers, as recorded in China. The attackers use publicly available user information.

Anatomy of *Backdoor. IRCBot.Dorkbot. A* Trojan attack

According to research conducted by *"Bit Defender"* company in May 2011, the number of attacks has increased by 83% when compared to other malware on the Internet. The *technical characteristics* of the aforementioned Trojan, which was discovered on May 5, 2011, are mediocre spreading, loss and small size (from ~ 118KB). Its method of spreading is via instant messaging using *MS MSN* or USB devices. The typical symptoms include the increased *HTTP* traffic, presence of hidden files in the file, while the filename is always generated by randomly chosen characters, and the presence of the following value in log files "*HKEY_CURRENT_USER\Software\\Microsoft\\Windows\\CurrentVersion\\Run\filename*".

It implements itself in multiple layers of (the) encrypted data. *Ntdll.dll* file checks whether the attacked computer's OS is 32-bit or 64-bit, and then generates *crc32* table. The c*rc32*table is used for decoding, and it consists of a structure, which contains information about the encrypted string, the string length and the hash function. Then, it enrolls in any open OS processes. Options *Delete File A/Delete File W, Move File A/ Move File W, Create File A, Send* are intercepted in the code and the information is taken from the buffer. In case the parameter value in the buffer is null or its length is less than 6 characters, the download and interception of information from the buffer are executed. Otherwise, the buffer is copied; *FTP* or *POP3* protocols are checked. So, if the buffer carries information that begins with *"user"* or *"pass",* the information is sent to a local variable. The distinction between these protocols is made by checking the existing specific FTP commands, such as "CWD", "PDW", "FEAT", "TYPE", "PASV". After making a decision, a message is sent:

1. For FTP, if "*ftp grab*" state is mapped on:

   "lenght_message.ftplog.ftp://user/password@network_address:hostshort p=_curent_module_file_name_ "

2. For POP3 if "*pop grab*" state is mapped on:

   "lenght_message.poplog.pop3://user/password@network_address: hostshort p = _curent _module_file_name_".

Http Send Request A/Http Send Request W option seeks information in the URL string. The goal is to download the login information of some computers to specific sites. First string searches the URL, the other represents optional information, and the third collects the name of the target server, as shown in the following example:

"*google.*/*Service Login Auth*"
and "*service=YouTube*" (target
"YouTube")"*google.*/*Service Login Auth*"
and "*Password=*" (target "Gmail").

When a pair is found, the search for username and password continues. Such data is recorded as a string, which makes it easier for the attacker to easily collect all the data necessary for the attack. Information is sent, if the filtering requirements are fulfilled, namely: *"cPanel", "WHM", "WHCMS", "Directadmin"*. DF is confronted with a difficult task of discovering the evidence. The reason for this is the so called *"Trojan defense"*. There is a dilemma, when the zombified computer is found, whether the computer is really corrupted, or the attacker has actually committed a crime from that computer. Therefore, finding and opening the source code root kit and the Trojan is very important, as previously described. Also, it is essential to establish running services, processes, and see if they can be associated with the installation of the root kit and the Trojan.

Forensic investigation experiment of a zombified VM

An attack on a VM was executed under the controlled experiment. While monitoring the network traffic by using *WireShark* forensic tool, it was noted that certain content was copied from one location to another. In particular, one client transferred a file to another client, which in this case simulated a virus (or Trojan). This activity was recorded and the follow-up began. When a forensic tool (Figure 2), recorded *eicar.zip* file during the computer monitoring, the process of monitoring communications between the users of these two machines began. *Eicar* file is sort of a *control virus* that should alert the antivirus software and check the level of OS protection, without doing it any harm. Figure 2 shows that a demand for copying the file has been made, and that the attack came from the IP address 192.168.99.118, which has been identified by the forensic tool as the source of this communication. The computer that monitors and receives this file is the destination machine and its IP address is 192.168.99.50. Relying on this information,

one can see that they are on the same network domain, as well as in some of the internal networks. The time when the original computer initiated the copy request can be seen. All the information from the source and destination computers is relevant for the forensic investigation, so that DF would know where to direct the investigation and track the timings which show when some activity occurred. In Figure 2, you can see the entire communication - from the time when the copy request was issued from the source to the destination machine. DF may use the binary inscription from *eicar.zip* as information, i.e. he can identify and prove the existence of a malicious file using a hard drive from the tested computer, with the assistance of the hexadecimal editor. Path to the computer file, or more precisely, the place where it will be copied, can be seen in Figure 2. This is important information that will reduce the DF's investigation time, and prevent the suspect from manipulating or applying the anti-forensic activity on the file - evidence that is incriminating at this point. Figure 2 also shows that Wire Shark-forensic tool recorded the used protocol and that it can perform filtering of the entire traffic. For instance, it can separate only the TCP communication.

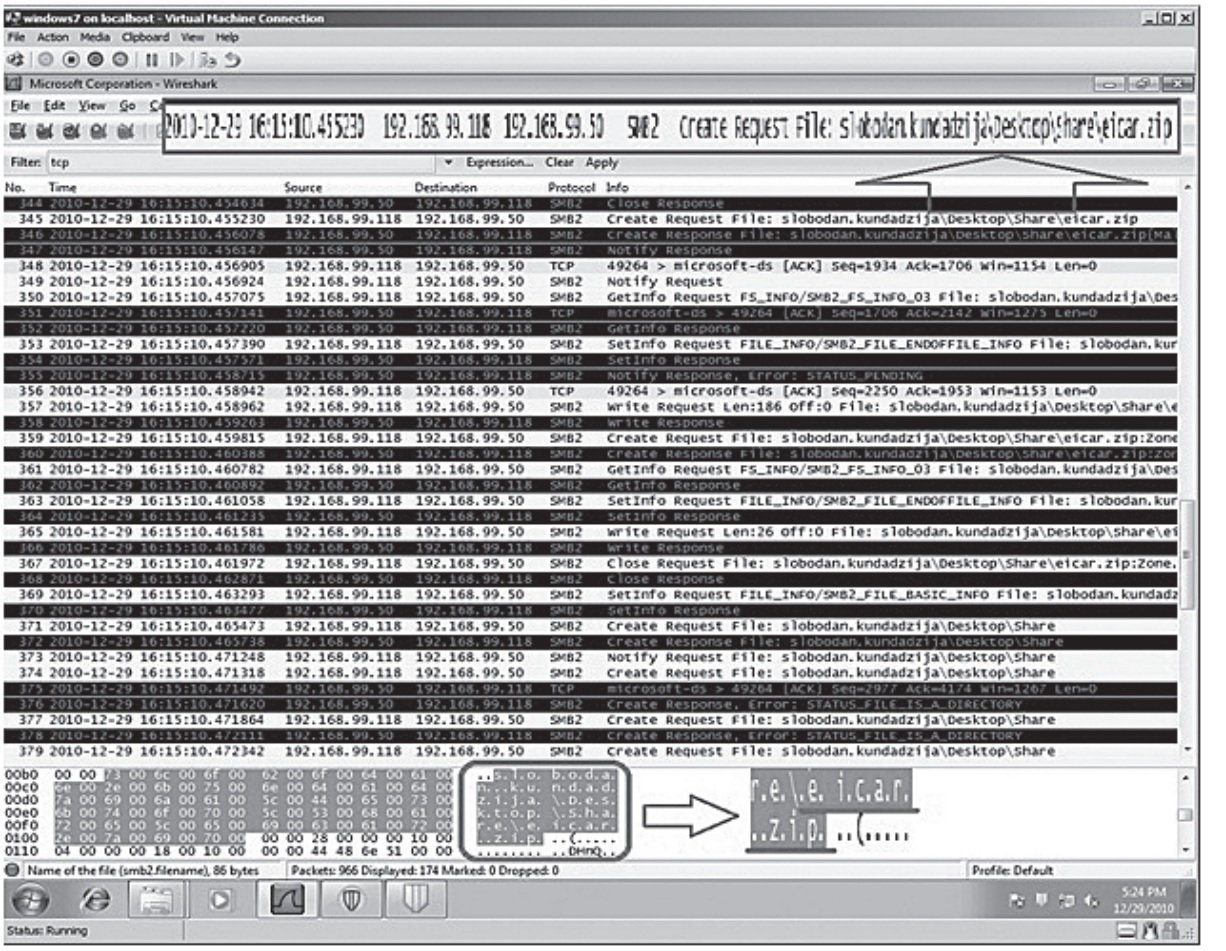

Figure 2.

Forensic investigation of the zombified VM was carried out in experimental verification and the evidence to incriminate the attacker was found, i.e. "Trojan defense" by VM owner was proved and DF's deception was prevented. The attacker uses physical computers (Figure 1) to attack from the outside and through social engineering, passing malware on the VM. The study found that Trojans were delivered through pictures infected with malware and attached to an e-mail.. After that, the attacker starts copying the Trojans to VM.

Forensic investigation of a zombified VM was carried out in experimental verification and the evidence to incriminate the attacker was found, i.e.

"Trojan defense" by VM owner was proved and DF's deception was prevented. The attacker uses physical computers (Figure 1) to attack from the outside and through social engineering, passing malware on the VM. The study found that the Trojans were delivered through pictures infected with malware attached to an e-mail. Unknowingly, by downloading the attachment, the curious user runs malware, thus enabling the attacker to open the rear door. After that, the attacker starts copying the Trojans to the VM. Such activity is recorded by the *WireShark* forensic tool, as shown in Figure 2. The information about IP addresses is taken from the hexadecimal and binary inscriptions from Trojans called *"eicar"*. The Trojan file is in the form of a zipped file. After DF accessed the corrupt VM, the *"eicar"* file was found, whose binary values were compared to those in Figure 2. The identity was proved and the file becomes digital evidence. By opening the Trojan's source code, paths used to send information to the attacker were found. By comparing the downloaded information taken from the file with the information from the monitoring, it was determined that it is the same computer. The attacker tried to defend himself by removing the evidence, deleting the file from the zombified computer, but all data was saved owing to the functionality and the structure of the virtual hard disk of the corrupted machine. The corrupt VM has infected all VMs in the domain with malware that spread through the Internet. The host remained uninfected. Further investigation revealed that the attacker entered domain from the physical machine by stealing the username and password through social engineering.

Protective measures

Examples of malware attacks are diverse. Few more possible attacks on the VMs have been experimentally verified. The greatest risk is in insufficient user's awareness of the nature and degree of modern malware sophistication. In order to enable effective protection, it is necessary to update the antivirus (AVP) on a daily basis and scan regularly the computer using AVP based on digital signature and heuristic checks of the familiar malware. Ports, previously closed by the AVP, should not be opened, which is a basic measure of protection that many users ignore.

This could happen when some third party (site, application ...) asks the user to open a port to download, for example, some multimedia content from the Internet. The next protective measure is to check the authenticity of the advertiser on the Internet that offers free applications from expensive branded manufacturers in the promo period, because in most cases, the malware distribution and the attack stand behind such offer. With the use of an electronic mail, one should always check the authenticity and validity of the sender before downloading. The reason for that is the wide availability of social networks such as Twitter, Facebook etc. The attacker has the opportunity to gather information from social networks and mimic close friends, relatives, acquaintances, thus committing fraud and crime (for example - distribution of malware). It is also recommended to scan all removable media connected to the computer. One should bear this in mind when using one's own portable media on public computers. Special attention should be paid to computers that are available to large numbers of people, computers that are used in public sectors or those located in companies' sectors which are used by a large number of users, without any arranged or implemented system of protection and security.

Into such computers, the attackers usually insert malware that could be transferred to any portable media. When the media is connected to an infected public computer, it will download malware and it will automatically become "infected". An example for that could be a photo station for quick development of pictures located in a shopping mall.

CONCLUSION

The conducted experimental research and analysis verify the fact that the abuse and anti-forensic activities in the virtual environment cannot always be controlled, but can be prevented. When they occur, they can cause a huge material and moral damage to an individual and the society in general.

The absolute safety in the virtual environment cannot be provided. Hence, we must take into account the human factor. In this paper, we have experimentally proved that it is possible to fight against malware in the CC. It is necessary to be conversant with the following: design and programming, because the current malware is written in a

sophisticated code; network engineering, because malware spreads through both public and private networks; web programming, since it is placed on sites in a form of traps; digital forensics, in order to discover the evidence and, finally, the constitution and the laws of the country in order to apply the laws on individuals that violate it. Good cooperation between the DF and CC provider is needed, as well as uninterrupted monitoring of delivery quality of CC services. The importance of virtualization as a tool for forensic investigation is that a VM can be used to simulate a malware attack, because all malware remains in the VM, while the physical machine - the host, is completely safe. Therefore, the forensic investigation and presentation of evidence can be simplified. Also, it is easier to prove and reconstruct the attack in the court. By creating a number of independent VMs in CC, DF is able to use them as workstations and the evidence can be placed on virtual hard disks. The CC environment allows DF to avoid carrying removable media for storing evidence, devices, workstations, etc., in the field. It is enough for them to have a mini-notebook or any device that has an internet connection, and upon authentication on the VM via remote desktop; they can access their "virtual" workstation. Thus, they are given the possibility to transfer the data and evidence to virtual hard discs. Any new knowledge and solutions in the field of digital forensic investigations in the virtual environment can make a significant contribution to solving the potential cases of computer crime in the CC environment.

REFERENCES

Anti-forensic tehniques. Wiki [online]. Available from: http://www.forensicswiki.org/wiki/Anti-forensic_techniques [accessed 6 August 2012].

Barrett, D., Kipper, G. (2010) Virtualization and forensics: a digital forensic investigator's guide to virtual environments. Burlington, MA: Elsevier.

Carr, J. (2007) AntiForensic methods used by Jihadist web sites [online]. Available from: http://www.esecurityplanet.com/prevention/article.php/3694711/AntiForensic-Methods-Used-by-Jihadist-Web-Sites.htm [accessed 12 August 2012].

Cloud Security Alliance (2009) Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. [online]. Available from: https://cloudsecurityalliance.org/csaguide.pdf [accessed 5 September 2012].

Denial of service attack. Wikipedia [online]. Available from: http://en.wikipedia.org/wiki/Denial-of-service_attack [accessed 17 July 2012].

Grubor, G., Njeguš, A., Ivaniš, N. (2011) Glavni faktori uticaja virtuelizacije tipa I na forenzičku istragu. 8. naučni skup sa međunarodnim učešćem Sinergija 2011. 25 March 2011 Bijeljina. Bijeljina: Sinergija University, 55-63. (in Serbian)

Grubor, G., Njeguš, A., Ristić, N. (2010) Paradigma zaštite distribuiranog računarstva. 6. naučni skup sa međunarodnim učešćem Sinergija 2010. 19 March 2010 Bijeljina. Bijeljina: Sinergija University, 176-184. (in Serbian)

Lillard, T., et al. (2010) Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data. Rockland, Mass.; Oxford: Syngress.

Man in the middle attack. Wikipedia [online]. Available from: http://en.wikipedia.org/wiki/Man-in-the-middle_attack [accessed 2 September 2012].

Mather, T., Kumaraswamy, S., Latif, S. (2009) Cloud security and privacy: an enterprise perspective on risks and compliance. Farnham : O'Reilly.

Milosavljević, M., Grubor, G. (2009) Digitalna forenzika računarskih sistema. Belgrade: Singidunum University. (in Serbian)

Milosavljević, M., Grubor, G. (2009) Istraga kompjuterskog kriminala : metodološko-tehnološke osnove. Belgrade: Singidunum University. (in Serbian)

Security response. Symantec [online] Available from: http://www.symantec.com/security_response/writeup.jsp?docid=2005-081910-3934-99 [accessed 5 July 2012].

Veinović, M., Ivaniš, N. (2011) Zloupotreba sertifikata u servisu elektronske pošte. Singidunum revija. 8 (2), 79-86. (in Serbian)

Virus encyclopedia. Bitdefender [online] Available from: http://www.bitdefender.com/resourcecenter/virus-encyclopedia/ [accessed 20 September 2012].

FORENZIČKA ISTRAGA „TROJANSKE ODBRANE“ U VIRTUELNOM OKRUŽENJU

Rezime:
U ovom radu prikazan je primer napada malverom na virtuelni računar. U napadu malvera veliku ulogu igraju greška ljudskog faktora i tehnike socijalnog inženjeringa.Nedovoljna edukacija korisnika o bezbednosti informacija, olakšava dalje delovanje napadača.Napadač piše kôd malvera po potrebi – kao *keylogger, downloader* itd.Svaki napad uključuje dobru pripremu, skeniranje portova, prikupljanje informacije o antivirusnim softverima i načinu korišćenja ciljnog računara, razmatranje scenarija napada, izbor prilike i metoda napada. U radu je razmatrana antiforenzička uloga trojanca u korumpiranom virtuelnom računaru sa kojeg je izvršena zloupotreba, bez znanja vlasnika. Opisana je eksperimentalna verifikacija forenzičkih aktivnosti za dokazivanje tzv. „trojanske odbrane“ u virtuelnom okruženju.

Ključne reči:
malver,
trojanac,
trojanska odbrana,
cloud computing,
virtuelna mašina.

Received: 06.09.2012.
Correction: 08.10.2012.
Accepted: 12.10.2012.