ANALYSIS OF MALICIOUS ATTACKS ACCOMPLISHED IN REAL AND VIRTUAL ENVIRONMENT

Dimitrina Polimirova, Eugene Nickolov

Abstract: In this paper an analysis of possibilities offered by virtual environments for accomplishing attacks to and within it, is made. Main techniques for accomplishing an attack to virtual environment are pointed and real virtual attacks and successful virtual attacks are examined. An analysis of accomplished attacks is made and percent distribution of real virtual attacks and successful virtual attack is graphically illustrated. Respective assessments and recommendations for future investigation are made.

Keywords: Virtual Machine Environment, Virtual Environment, Attack/Attack tools, Defense/Defense tools, Malicious Code

ACM Classification Keywords: D.4.6 Security and Protection: Invasive software (e.g., viruses, worms, Trojan horses)

Introduction

Computer Viruses, Worms, Trojan Horses, Backdoor, Rootkits, Spyware, Adware, etc. are terms used years ago mostly by computer specialists. However, now they present in daily speech not only of employments of corporate, academic and government organizations, but also of final users. Everybody knows less or more for their action and damages they can harm to the computer systems and information flows. The availability of various attack methods determines the necessity of investigation of different methods and means for defense of computer systems, networks and information flows.

A general strategy for protecting computer systems and networks could include using virtualization techniques to achieve increase in information security not only of information flows, represented by file objects, but also of operation system as a hole.

Since the 70-th of XX century the problem for security and protection of information flows has drawn developers' and constructors' attention in the area of information technology [1]. With the first malicious attack in the 60th of last century [2], investigations in the area of system protection receive financial support. As a result for a short time ideas decreasing the risk in the system management, are realized.

The aim and tasks

The aim, which can be set in this paper, is related to investigations of the set of possible virtual attacks and its reduction to the set of successful virtual attacks, which have specific behavior in Virtual Machine Environments (VMEs) to overcome its protecting mechanisms.

The main hypothesis will be related to the possibility to make analysis and estimation of different techniques for successful accomplishing of an attack to virtual environment.

The following tasks are set in reaching the aim:

1) to make analysis of Virtual Machine Environment as a possibility for accomplishing attacks to and within it;

2) to determine the set of real virtual attacks;

3) to examine the main techniques for accomplishing an attack to virtual environment;

4) to determine the set of succsessful virtual attacks.

The Problem

1. Virtual Machine Environment as a place for executing malware

1.1. Description of Virtual Machine Environment

Virtual Machine Environment (VME), mention also in this paper as virtual environment, gives the possibility to create one or more guest operating systems from one primary (host) operating system. Each created guest operating system works in emulated environment and it has controlled access to virtual and real hardware resources (Figure 1).

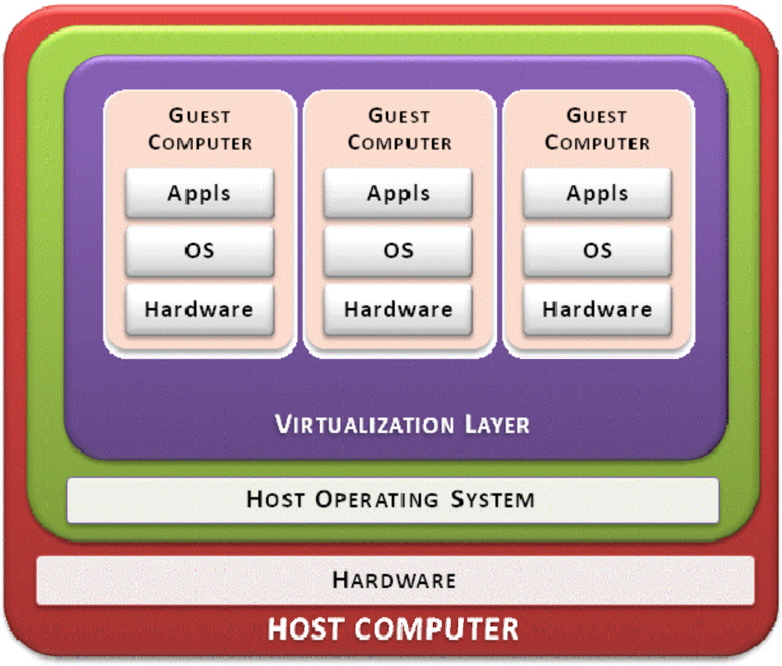

Figure 1 Virtual Machine Environment

1.2. Benefits of Virtual Machine Environment.

The increasingly using of virtual environments speaks for itself for the benefits, which can be obtained, namely:

(1) possibility for reducing the number of physical machines. This can be achieved by the possibility, which virtualization offers to integrate several servers into one hardware platform. This way expenditure for hardware can be drawn;

(2) easy management. The management is from one physical place by one person. We can see here the economic benefit with respect to the human resources, but more important is that one person, which is

specialist has an access to the management of real and all virtual environments. This way the possibility to harm the system by someone through carelessness or through ignorance is decreased significantly;

(3) increasing the security. The virtual environments are exposed to attack as real environments. Since the virtual environments are identical to real one, they are friendly place for distributing of malicious software and accomplishing of attacks. Not every employee in one organization has enough experience and knowledge to succeed to protect itself from such types of attacks even though most of the employees are more or less familiar to the main actions for protecting of malicious software. From the point of view of the primary operating system, the virtual environment can have a defense role. All events occurred in the virtual environment are separated from the real environment. In the most cases if the malicious software gets into the guest operating system, it continue to thrive there while the primary operation system, host computer and even other virtual machines stay clean;

(4) possibility to load different operation systems on one hardware platform. This technique is often used by computer specialists in the processes of building and testing different software. Different computer system and networks configurations are simulated. If there is a program bug, the host operation system leaves unaffected;

(5) possibility for easy and fast recovery of critical applications. In case of system crash the virtual environment gives the possibility for fast and easy recovery not only of critical applications, but also of the whole system.

1.3. Virtual environment in the practice

In most cases virtual environments are used by software vendors during the processes of software building and testing. This technology can take place in the work of different sphere, of course - individual users, businesses, government agencies, and academic institutions. For the aim of this paper only the virtual environments application in the work of security and defense vendors on the one hand, and malicious code vendors on the other hand, will be examined.

Using the virtual environments became so popular that hackers direct their attention to them. Attacks, accomplished to virtual environment, are investigated not only by the vendors of security and defense software, but also by the vendors of malicious codes.

Vendors of antivirus and security software use virtual environments, to examine the behavior of different types of attack tools without damaging the real environment. After that the respective defense tool can be built.

On the other hand vendors of malicious code use virtual environments too to test if their attack tool works appropriately and can accomplish its planned action in different computer, system and network configurations.

The virtual environment is that which consolidate the both sides – used by ones to protect, and by others – to attack. In this connection the main goal of the vendors of malicious codes is to detect the presence of virtual environment and if they detect one – to change their action.

1.4. Virtual Machine Environments software

Figure 2 shows comparison of the most widespread virtual machine emulators used by hackers.

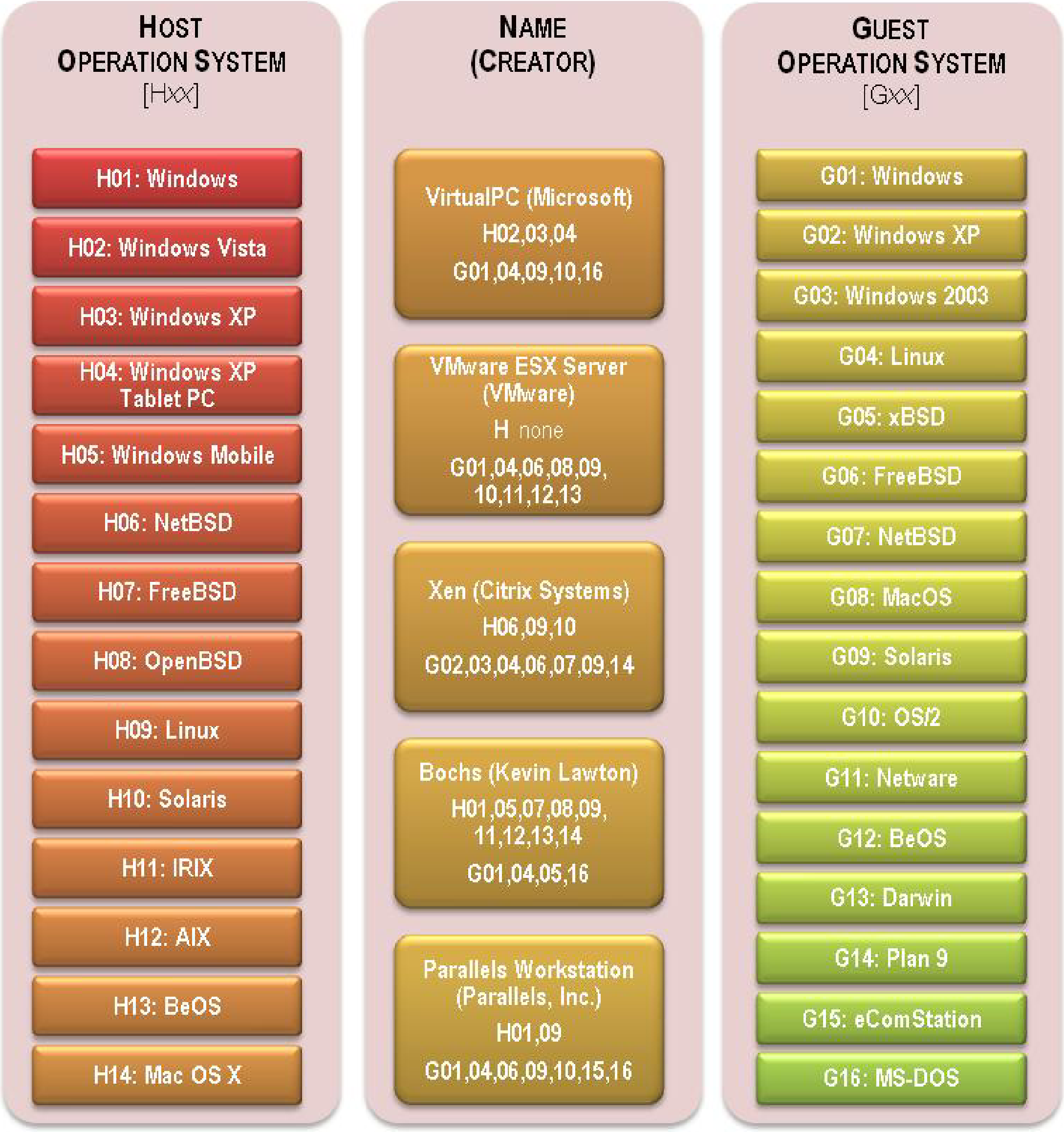

Figure 2 Widespread virtual machine emulators

2. SETS OF POSSIBLE VIRTUAL ATTACKS AND SUCCESSFUL VIRTUAL ATTACKS

2.1. Analysis of the set of possible virtual attacks

As a hole the attacks can be presented by malicious software and malicious attack. In case of malicious software the direct participation of a user at the moment of the attack is missing, while in case of malicious attack the user's presence is required. [3], [4].

The variety of attack tools for the recent years is big. They can be terminologically divided into two main categories: malicious software (malware) and greyware (grayware). In the set of possible virtual attacks are included attack tools, used successfully or not to accomplish attacks within/to virtual environment. The set of successful virtual attacks includes 11 basic (the most popular for 2008) attack tools (9 for the group of malware and 2 for the group of greyware), separated in 4 groups respectively 3 for malware and 1 for greyware (Figure 3). The chosen attack tools are generalized from the most frequently used attack tools in the recent years [5].

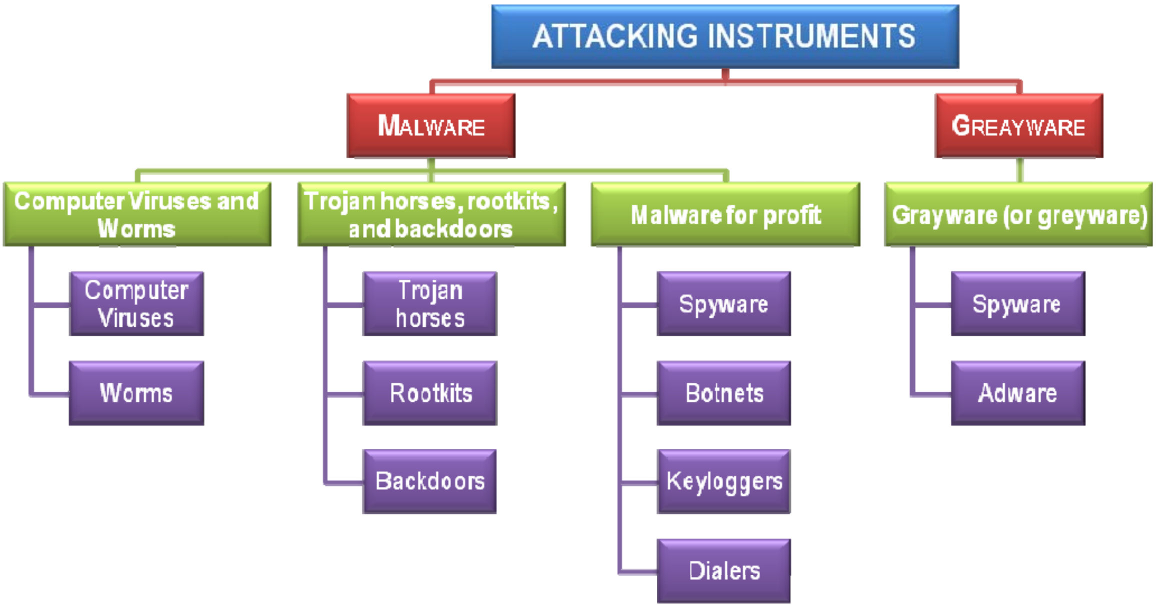

Figure 3 Attack tools included in the set of possible virtual attacks

2.2. Main techniques for accomplishing an attack to virtual environment

According to security software vendors the main attacks, accomplished to virtual environment, are three [6]:

1) the goal of the first type of attack is to detect the presence of virtual environment;

This is the most widely spread attack to VMEs and it is in pawn in the attack tools' scenarios. The goal of the attacks is to determine the presence of virtual environment. If such is found they change their behavior. In the common case of detecting virtual environment malicious code stops its activity. That way the vendors of antivirus and security software can't easily analyze the malicious code and building the respectively protection tool is hard and more slowly.

Figure 4 shows several techniques for detecting the presence of virtual machine environment [7]. These techniques are used by different attack tools from the groups "Computer Viruses and Worms", "Trojan horses, rootkits, and backdoors", "Malware for profit", and "Grayware (or greyware)" (for example: SubVirt, Confiqer, Vundo, Agent.FDS, Banking.G, OscarBot.UG, Socks, Aresas.a@MM, CodeRed, etc.).

2) the second attack consists in the possibility of the malicious code to accomplish DoS attack to VME, which will force the virtual machine to exit;

Usually the attack tool has a vulnerability scan. If the malware founds vulnerability it executes the exploit in Virtual Machine Environments. After that a Denial-Of-Service attack can be accomplished. That technique is used by ByteVerify, MS09-033, etc.

3) the third attack consists in the possibility of the malicious code to dismiss the virtual machine protecting environment.

In this case the attack needs to completely dismiss the virtual machine protecting environment and to continue its action. As far as I know such malicious codes don't exist.

Mentioned above malware' names are chosen from the information database of National Laboratory of Computer Virology – BAS as the most frequently accomplished in Bulgaria, Balkan Peninsula and south-east Europe.

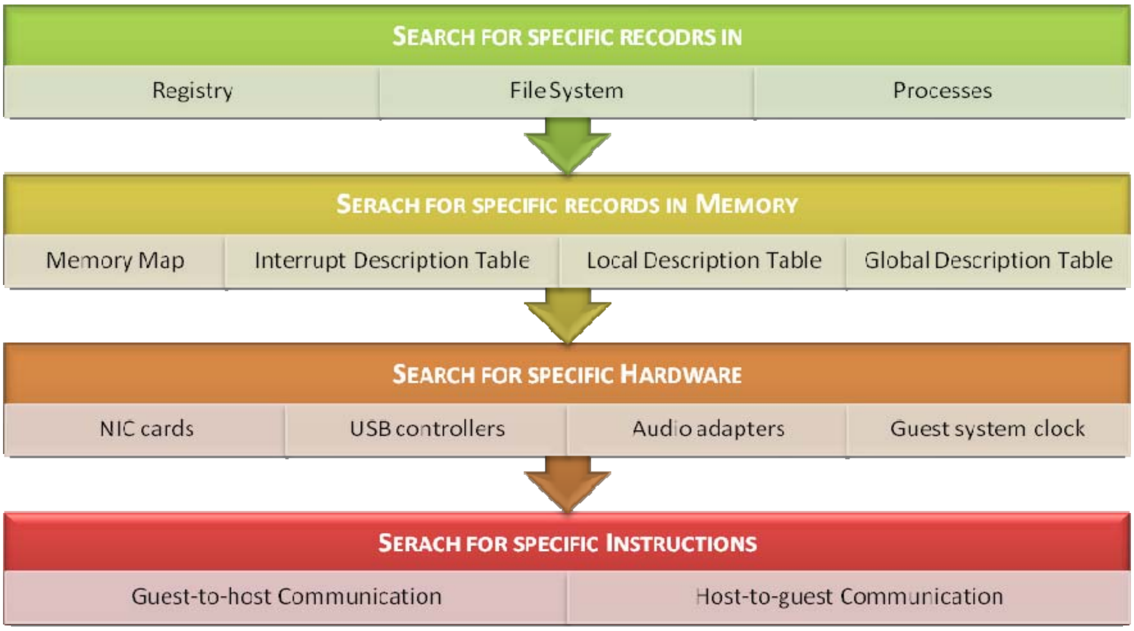
SEARCH FOR SPECIFIC RECODRS IN
Registry
File System
Processes
SERACH FOR SPECIFIC RECORDS IN MEMORY
Memory Map
Interrupt Description Table
Local Description Table
Global Description Table
SEARCH FOR SPECIFIC HARDWARE
NIC cards
USB controllers
Audio adapters
Guest system clock
SERACH FOR SPECIFIC INSTRUCTIONS
Guest-to-host Communication
Host-to-guest Communication

Figure 4 Virtual Machine Environment Detection Techniques

2.3. Analysis of the set of successful virtual attacks

More and more attack tools includes in their code possibility to attack virtual environment. Most tools heaving such a technique are Trojan Horses, Worms, Rootkits, Backdoors, Downloaders and Spyware.

The set of successful virtual attacks includes attack tools that can accomplish an attack to virtual environment. The set of successful virtual attacks includes 7 basic attack tools (6 for the group of malware and 1 for the group of greyware), separated in 4 groups respectively 3 for malware and 1 for greyware (Figure 5).

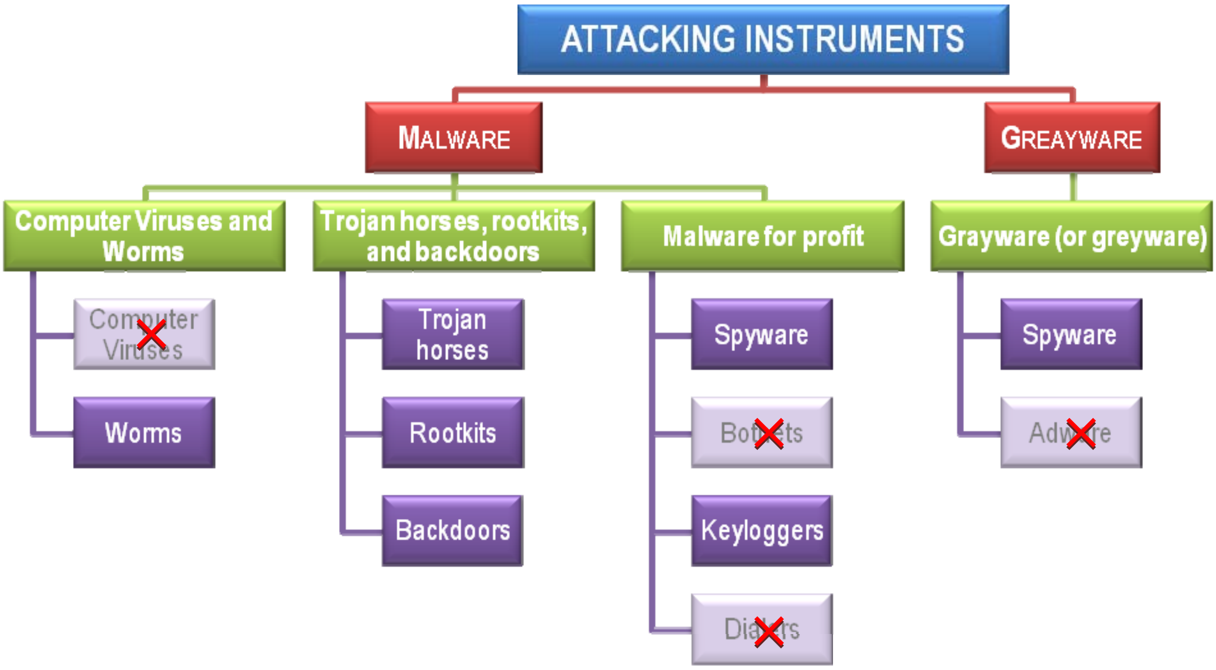

Figure 5 Attack tools included in the set of successful virtual attacks

Figure 6a, b, c, d, e, f shows graphically the percent distribution of the mentioned above attacks, accomplished in Bulgaria, Balkan Peninsula and south-east Europe for 2008. Graphics shows also the percent distribution of the attacks from the set of possible virtual attacks (RE) in relation to respective attacks from the set of successful virtual attacks (VE). The data are collected from the current information base of National Laboratory of Computer Virology of Bulgarian Academic of Sciences.

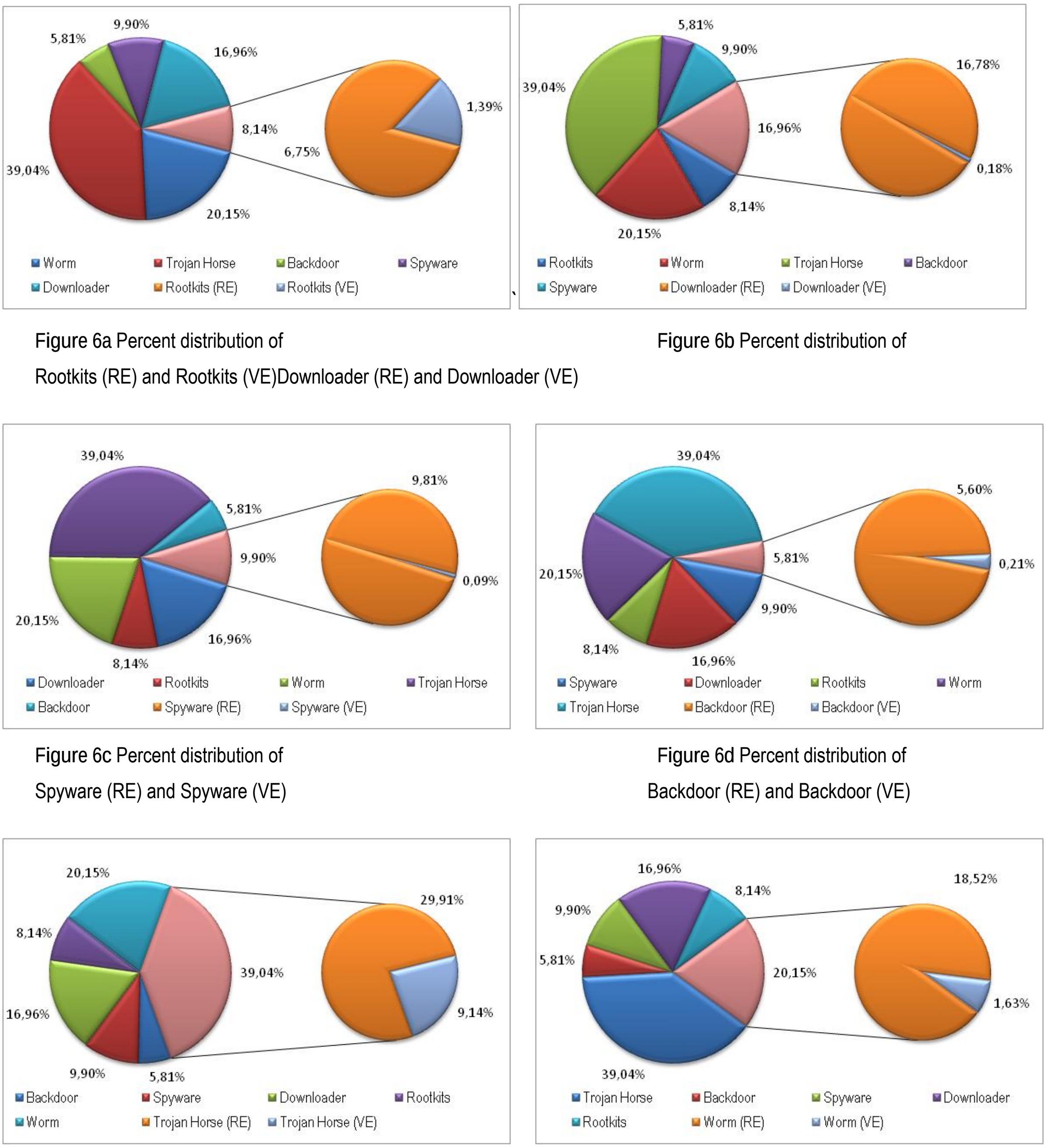

Figure 6a Percent distribution of

Figure 6b Percent distribution of

Rootkits (RE) and Rootkits (VE)Downloader (RE) and Downloader (VE)

Figure 6c Percent distribution of
Spyware (RE) and Spyware (VE)

Figure 6d Percent distribution of
Backdoor (RE) and Backdoor (VE)

Figure 6e Percent distribution of
Trojan Horse (RE) and Trojan Horse (VE)

Figure 6f Percent distribution of
Worm (RE) and Worm (VE)

Figure 6 Percent distribution of the attacks from the set of possible virtual attacks and their corresponding attacks from the set of successful virtual attacks

Assessments and Conclusion

1) With respect to the virtual environment, one might say that they are a good precondition for development of new attack techniques, which can be in pawn in the malicious scenarios of the attack tools. Virtual environment can be used not only by the vendors of security software, but also by the vendors of malicious code.

2) With respect to the different techniques for attacking virtual environment, one might say that they are much and in the most cases the goal is to detect the presence of virtual environment.

3) With respect to the set of possible virtual attack, one might say:

3.1) the chosen types attack tools are appropriate for conducting analyses and making assessments;

3.2) attack tools can be used within virtual environment, but not each one has the possibility to accomplish attack to the virtual environment.

4) With respect to the set of successful virtual attack, one might say:

4.1) there are representatives from all groups of attacks and only a few are dropped down (as Computer Virus, Botnets, Dialers, and Adware);

4.2) the number of dropped down attack tools is only around 36% and one might say that the hackers are interested in using techniques for attacking virtual environment.

5) With respect to the made investigations for the percent distribution of the attack from the set of possible virtual attacks in relation to respective attacks from the set of successful virtual attacks, one might say that 17,08% of Rootkits, 1,06% of Downloaders, 0,91% of Spyware, 3,61% of Backdoors, 23,42% of Trojan Horses, and 8,09% of Worms has the possibilities to accomplish an successful attack to virtual environment.

Future analyses and investigations can be made with respect to the examination of the economical expenditure of providing security policy for different computer, system and network configurations in real environment in comparison with virtual environment.

Bibliography

[1] Denning, D., A Lattice Model of Secure Information Flow, Communications of the ACM, v. 19 n. 5, May 1976, pp. 236-243

[2] Trigaux, R., A history of hacking, (http://www.sptimes.com/Hackers/history.hacking.html)

[3] Shaw, W., Cybersecurity for SCADA Systems, PennWell Corp. (2006), ISBN-13: 978-1593700683, p. 194

[4] Radhamani, G., Rao, R., Web Services Security and E-business, Global (2007), ISBN-13: 978-1599041681, p. 115, p. 25

[5] Nickolov, E., Modern Trends in the Cyber Attacks Against the Critical Information Infrastructure, Regional Cybersecurity Forum, 7-9 October 2008, Sofia

[6] Ferrie, P., Attacks on Virtual Machine Emulators, Symantec Advanced Threat Research, (http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf)

[7] Liston, T., Skoudis, E., On the Cutting Edge: Thwarting Virtual Machine Detection, (http://handlers.sans.org/tliston/ThwartingVMDetection_Liston_Skoudis.pdf)

Authors' Information

*Dimitrina Polimirova, PhD, Research Associate, National Laboratory of Computer Virology,
Bulgarian Academy of Sciences, Phone: +359-2-9733398, E-mail: polimira@nlcv.bas.bg .*

*Prof. Eugene Nickolov, DSc, PhD, Eng, National Laboratory of Computer Virology,
Bulgarian Academy of Sciences, Phone: +359-2-9733398, E-mail: eugene@nlcv.bas.bg .*