International Journal of Digital Information and Wireless Communications (IJDIWC) 1(3): 645-650
The Society of Digital Information and Wireless Communications, 2011(ISSN 2225-658X)

Investigation of Malware Defence and Detection Techniques

Farid Daryabar
Asia Pacific University College of Technology and Innovation
Technology Park Malaysia Kuala Lumpur, Malaysia
farid0fx@yahoo.com

Ali Dehghantanha
Asia Pacific University College of Technology and Innovation
Technology Park Malaysia Kuala Lumpur, Malaysia
ali_dehqan@ucti.edu.my

Hoorang Ghasem Broujerdi
Asia Pacific University College of Technology and Innovation
Technology Park Malaysia Kuala Lumpur, Malaysia
hoorang@ucti.edu.my

Abstract—Malwares are considered as a major threat vector which can be potentially caused huge damage to both network infrastructure as well as network applications.

In this paper, different techniques such as repacking, reverse engineering and hex editing for bypassing host-based Anti Virus (AV) signatures are illustrated, and the description and comparison of different channels and methods when malware might reach the host from outside the networks are demonstrated. After that, bypassing HTTP/SSL and SMTP malware defences as channels are discussed. Finally, a new malware detection technique base on honeynet systems is discussed and its strengths and weaknesses were highlighted.

Keywords: Malware defences, Bypassing malware, Honeynet, Anti Viruses, Penetration Testing.

I. INTRODUCTION

Nowadays, almost every organisation depends on information such as financial, political, etc. By using the Internet protocols these information are transferred through the Internet and almost all internal networks are connected to the Internet directly or indirectly. In the internal networks there are many important systems such as Supervisory Control and Data Acquisition (SCADA) and bank databases, etc [1].

The term malware, which is also called malicious code and malicious software, refers to an executable file or application that are covertly injected to systems. Malware can be Trojan horses, Rootkits, and Backdoors. The main purpose of the malware is compromising the systems' Confidentiality, Integrity and Availability (CIA) [1].

Malware is executed on the internal networks and it provides full controlling the systems by its author when it is on the victim systems. Attacks with malware are the most expensive incidents for the companies and organisations [2].

In general, AV products detect malware in two methods, which are listed below:

1) Signature-based
2) Behavioral based

Signature-based works on the byte or binary patterns, and hashes of the known malware and hashes are saved in a large database of the AV products [3]. The result of comparison between the database of signatures and a program shows that the program is a malware or not [3]. False-positives in the comparison are almost impossible because the signatures are unique[4]. Malware creators often create various versions of a malware to avoid detecting them from AV signature-based method. Therefore, difficulty of the method is egregious when a new version of the malware is created. To prevent the problem, AV vendors utilize generic signatures [4]. Generic signatures method attempt to recognize the whole families of the malware, e.g. by creating a signature for a code segment that is shared by different versions of a malware [4].

Behavioral based detection methods recognize malware either by looking at the codes earlier than it is run or the AV runs it on a virtual sandbox environment to find a malicious activity [4]. By utilizing these methods, it is not needed to have a big database of binary patterns and hashes because the malware is simply recognized by its behavior. Occurring false positives in these methods are more common; therefore, these techniques are not often used [5]. Examples of these activities or behaviors are injection into privileged processes, alteration of critical operating system (OS) or AV files and keystroke logging [5].

Study about bypassing the malware detections considers on protecting the companies' systems. The consideration is based on the functionality of the malware that it cause the malware changes itself to prevent of detection. After that more researches about how to change existing malware to bypass detection have been done [5]. When a specimen malware has been found, the AV vendors can realize a signature or behavior show in the malware by analyzing the malware. To change existing malware to bypass AVs products, attacker is able to find the signature and the behavior, which AV vendors have realized, and then the attacker changes the malware to bypass the defences. Therefore, here AV vendors provide advantages for the attackers [5].

At first, the power rates of AV defences to recognize malware and changing malware's signatures in order to pass the AVs and the gateways are discussed. Then, bypassing 41 AV's programs by simple codes and description of how to detect malware before the malware gets in to the host are given. At the end, because of writing a new malware is the

best way for detection prevention by defences, we survey a detection system base on honeynet for organization to detect unknown malware before the malware reaches to their private networks.

II. REVIEW OF RELATED WORKS

Many companies' employees use unknown sources in Internet and they download executable files, which might be malicious files. The reason of preventing these activities by security administrators in companies is given and it is shown that how new malware or an existing malware, which is changed, might be pass by AV engines [4].

The ability of AVs in detection of some malware is indicated and it is tested to determine how often the malware are recognized by standard AVs. All the malware, which are mentioned in this part, have been scanned in VirusTotal [4]. It is a free service from Hispasec Sistemas and VirusTotal site scans all uploaded files by using 41 AVs base on signature detection method and each AV has updated with the newest malware signature [4]. The result of detection is different between stored and executed malware, which respectively shows malicious behavior and signature; therefore, it is not always deduced from only stored files [5]. The example is a malware with a known signature, which has changed its codes. But when a malware runs, the malicious signature may re-emerge base on packet's nature [5].

There are two different situations that malware can be detected or bypassed. First, bypassing host-based AVs and second Bypassing from AV gateways [5], which are protecting a network. different ways that a malware might bypass host-based defenders is given below:

A. Known Signatures

Most of the solutions are based on signature detection [5]. This method of detection searches for string of characters in documents and executables and if a file's string is exactly matched with one of the stored strings in the AV database, the file will be presented as a malicious.

Studies about malware shows that 22.000 new malware released every day [7]. And for the signature-based detection method, it is needed to have very updated knowledge about the specific malware.

For example, a Trojan called Turkojan which is available from the hacker group's web site [7] is one of the dangerous and well-known trojan. It is one of the backdoors, which capture keystrokes, audio and webcams; it gets password hashes, it has ability to get access remote desktop on compromised host. Even Turkojan is one of the well-known malware, but some AVs such as Microsoft, Norman, TrendMicro and Symantec that miss the malware samples in VirusTotal are not able to detect it [8]. Therefore, the issue is there is almost impossible to detect all malware by AV engines [8].

B. Changing The Signatures

Most of the malware detectors detect malware from their signature; therefore, Signature modification in one of the ways of bypassing the AVs. At the first the malicious signature should be identified. The simplest way to find the malicious signature is remove some parts of the malicious file and test the resulting file to VirusTotal until the malware is not detected in VirousTotal, as long as a valid file header is kept [5]. This method can be used to take out the malware signature.

After extracting the signature stage, the signature should be changed. The best way of changing the signature is hex-edit the signature[9]. All 41 AV products in VirousTotal identify the backdoor Tini's signature with its hardcoded port. Tini listening port is 777, which is le61 in hexadecimal [5]. Therefore, there is a possibility to find the part and change it to port 443, which is 01bb in hexadecimal. This process is shown in Figure 1 and Figure 2.

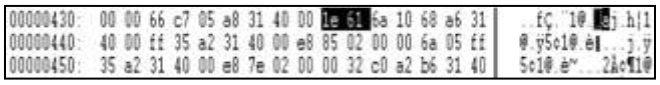

Figure 1: Finding the port number of Tini backdoor in hex-edit.

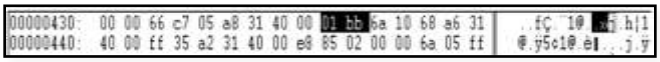

Figure 2: changing the port number in hex-edit.

At this moment, the new Tini should be uploaded in VirousTotal to check the bypassing rate [5]. As a result, in Figure 3 it is shown that almost half of the AV products have not detected the file.

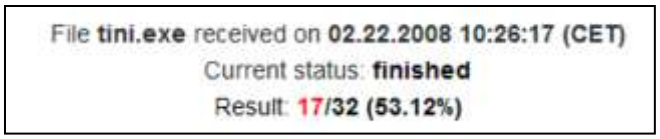

Figure 3: Detection result of new Tini in VirousTotal.

Another way for bypassing host-based AV products is to pack the piece of malware with a different packer [10]. This technique uses to pack an executable from simple XORing of the malware to compression and encryption hereof. And during the run time the malware will be unpacked. Some examples of packers include UPX, ASPack, Petite, Neolite and Themida [5].

C. Creation of New Malware

Another way of bypassing AV products is creating new piece of malware. The new piece of malware cannot be detected because it contains unknown strings that none of AVs are able to detect it and especially when the new malware is created simple by decreasing its suspicious

behavior. One of these kinds of malware was created by the author. It is proof-of-concept (PoC) piece of malware [5]. It is a backdoor receiving shell commands from the enemy through recursive DNS covert channel. In Figure 4 it is shown that the malware bypassing all 41 AV engines.

Figure 4: The result of bypassing new malware in VirusTotal.

The most significant consideration part should be detecting malware before it gets to a host inside a network. To reach this goal, implementation of SMTP and HTTP/SSL AV gateways has been considered in many companies [5]. The traffics from inside the companies towards the Internet must bypass through these gateways and these gateways have extra layer of security that the attackers should bypass them.

D. File Formats

Normally, all SMTP and HTTP/SSL AV gateways allow filtering by file format and as it is shown the custom-made malware was not recognized on the host, for example, the malware that was created by the author was not detected by all 41 host-based AVs [5]. In addition, creating a malware by a format like WSF makes the malware to bypass SMTP/HTTP AV gateways. This is illustrated in Figure 5 and 6, which respectively are result of custom EXE and custom WSF malware.

As it is shown in the diagrams, WSF increases 28 percent the success rate of bypassing SMTP gateways compare to EXE.

Consequently, the organisations use black listing, which finds a list of file formats that AV gateways does not allow and it is contrary to white listing. This option is great from security point of view.

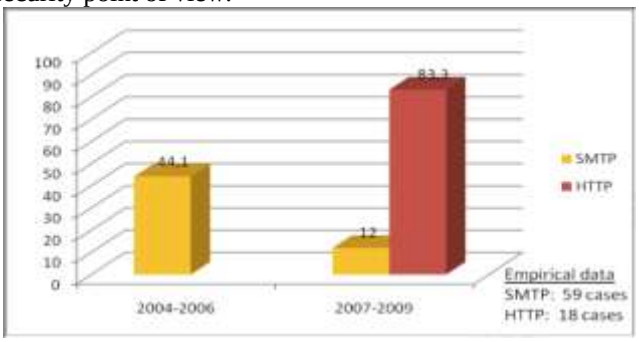

Figure 5: Percentage of AV gateways bypassed via custom EXE malware

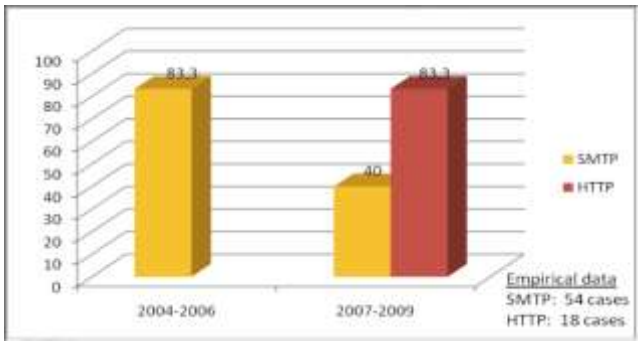

Figure 6: Percentage of AV gateways bypassed via custom WSF malware

E. Renamed Malware

Another method for bypass AV gateways is renaming the malware extension, but changing the extension need to be back in its original format when the file gets into the victim [5]. And simply may ask the user to change the file extension by some social engineering methods.

However, this kind of attack depends on how strong the AV is. Some magic byte recognitions look at the files' header rather just looking at the files' extensions. Figure 7 shows a custom EXE malware that its extension changed to XYZ and it shows 16,6% point increased in bypassing SMTP AV gateways.

At the end, renaming file extensions and manipulating the file header is the best improvement for bypassing the AV gateways.

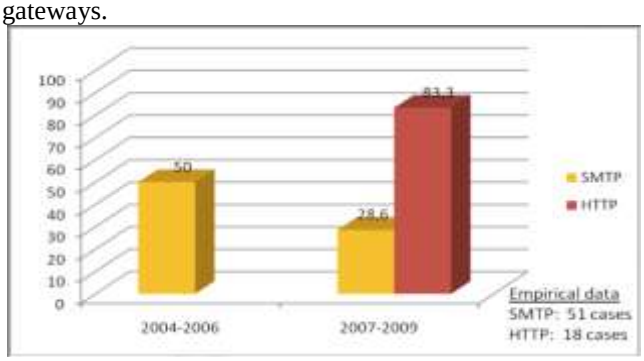

Figure 7: Percentage of AV gateways bypassed via custom EXE malware with renamed file extension

F. Compressed Malware

Another method to bypass the AV gateways is compression. A well-known malware named SubSeven, which is known by all AV engines, is tested in this part [5]. Figure 8 shows that the result of the malware before compression. When the malware compress with normal ZIP compression, the chance of bypassing the AV gateways increase 5-10 percent points, which is shown in Figure 9. Then, Figure 10 illustrates that the same compressed malware with password protection. Protecting the malware with password makes the chance of bypassing the SMTP defences by 20.5 percent points and 38.9 percent for HTTP

defences. Base on these discussions, AV gateways do not check the content of the files that are protecting with password and mostly they are encrypted. To protect the company from these kinks of attacks, the AVs should deny the password-protected files. These days companies improve their security by denying different kinks executables, but about password-protected files many of companies allow to pass the files [8].

Figure 8: 100% success rate in detecting SubSeven Trojan

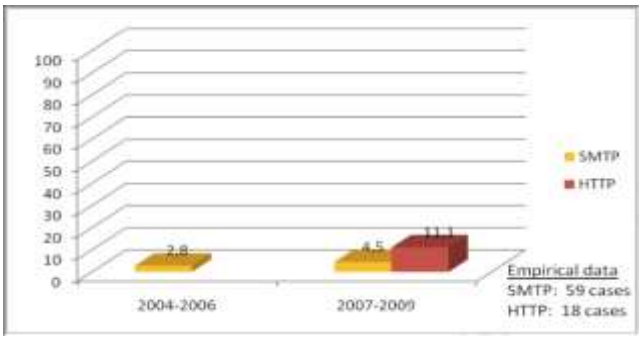

Figure 9: Percentage of AV gateways bypassed via known malware in ZIP archive.

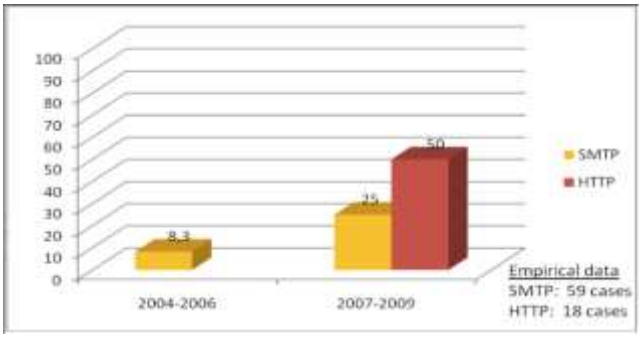

Figure 10: Percentage of AV gateways bypassed via known malware in password-protected ZIP archive.

To protect the companies' systems from the password-protected files, first the defenders should be aware of these kinds of password-protected files. Some of the most important compression formats are 7z, ace, iso, tar, taz, tbz, zip, rar, rev, img, lha, lzh.

G. Embedded Malware

Here is another way to bypass AV gateways named embedded malware. When a piece of malware is added into other files like documents, it decrease the percentages of bypassing defences [5]. Here Microsoft Office PowerPoint, Excel and Word documents are utilized to show these kinds of attacks. For these kinds of formats, many executable files are allowed to be attached as "objects" into the documents. When these embedded malware reach into the victim system, it is simply needed that the user opens the document and click on the object. Using SubSeven malware, which is embedded into a word document, increases 28.6 percent point for SMTP defences and 50 percent points for bypassing the HTTP defences.

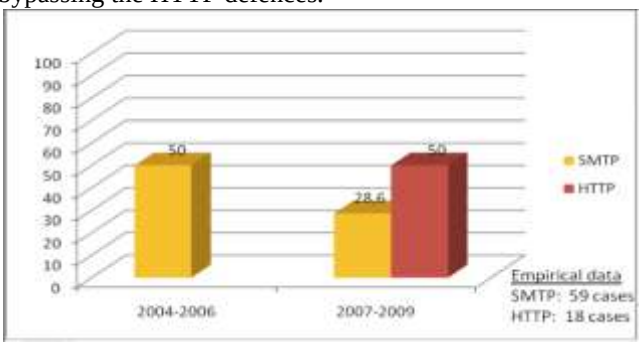

Figure 11: Percentage of AV gateways bypassed via known malware in MS Word document.

Base on the discussion, there is a possibility that MS office file contains malicious executable file. Some important formats that should be scanned or denied by the defenders are doc, docm, docx, csv, dot, dotm, dotx, iqy, odc, odp, pot, potm, potx, ppa, ppam, pps, ppsm, ppsx, ppt, pwz, elm and xls [5].

H. Encryption

For attackers, encryption is another method to bypass the AV gateways because the AV gateways are not able to go through the encrypted files. These kind of attacks are divided by 3 different kinds of attacks. First, Self-decrypting encrypted executables, Encrypted data files, Encryption inside applications. Consequently, encryption methods inside popular applications are one of the best ways to bypass and hide the malware.

I. Steganography

The definition of steganography is hiding some files, images or messages in side another files, images or messages[11]. Here hiding a piece of malware using steganography is used. SubSevem malware is hide inside a BMP picture and the Figure 12 shows the percentage rate.

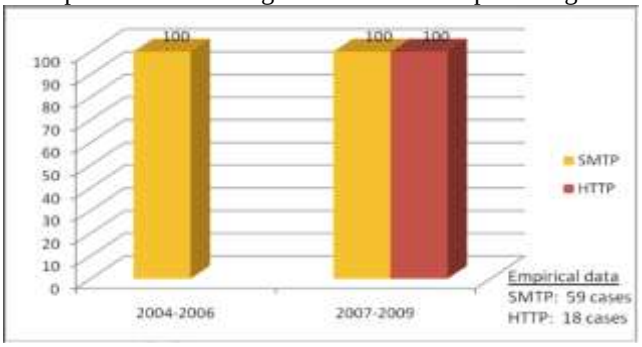

Figure 12: Percentage of AV gateways bypassed via known hidden malware in BMP picture.

As it is shown in the diagram, there is no way for the AV engines to detect these kinds of attacks. As security point of view it sounds dangerous and at the same time it is not that usable for the attackers because when the malware inside a picture reaches the victim, the malware needs to be extracted with the same steganography tool by the user [5]. This is only is the best way to passing the malware to the victim, but it is not automatically run by it self.

In general, honeypots are some systems that are designed to be traps for intruders and attackers, and honeynet is a network of different honeypots. Honeypots can be implemented as a firewall, IPS/IDS, to monitor systems and other security systems [12].

The main purpose of creating a honeynet is to gather information about the attacker's behaviors. The honeynets are simulation of the real network, for example, the same applications and services are provided in the honeynet [13]. Honeypots can be classified based on their deployment and based on their level of involvement [1]. There are two different honeypots base on deployment, production honeypot and research honeypot. Production honeypots just capture only limited information, and they are utilized in companies. Research honeypots have more complexity to implement and maintain, and they capture extensive information and researchers, military, or government utilize them [1].

III. PROPOSED SOLUTION

As it is explained, there is no reliable detection system to recognize malware and even AV products might miss the malware. Therefore, any incident handler or security administrator should analyze all activities of programs and services. By using traditional way, there are many logs and services that the incident handler should sift and analyze them. In other hand, detection tools are not able to recognize malware when there is a new and unknown malware.

The proposed solution is utilizing a new system which detects the new and unknown malware base on their behavior to protect the companies' systems and networks. a The new system is able to gather specific information of malicious activities by allowing the malicious codes to have access to the new detection system.

The detection system can be implemented in the companies as a honeynet system which requires three different levels of honeypots, and each honeypot has it own responsibilities. At the first, a honeynet system, which can be consider as Intrusion Detection System (IDS), will check the received data, which can be executable files, activities from outside the companies. It runs the received files in order to capture their activities and their behavior. It looks for the activities which might cause compromising the system. The activities such as services crashes, users complaining of slow access to hosts on the internet, program running slowly or not running at all, unknown processes, unusual and unexpected port openings (typical for Trojan horses and backdoors), corruption or lack of access to files, port scans and failed connection attempts targeted at the vulnerable service filenames with unusual characters, configuration changes disabling of security controls such as antivirus software and personal firewalls [1] should be considered. The first honeypot checks these activities and it gathers information about the malicious behavior. After finding any malicious activity, the honeypot system sends the information to the second honeypot. Then, the second system checks the running processes and it checks them with the AV engines. If the malicious program is found in the AVs engines, there is a known malware and the system prevents the data to enter to the companies' networks.

If AVs are not able to detect any malicious code from the data, it shows that the received data or files are unknown malware. Therefore, an unknown or new malware will be detected by deploying such systems.

After finding the malicious code, the honeynet systems can stop or delete the malicious program and they can prevent the new malware of getting access through the companies networks to a specific host that maybe a user who was trying to download the executable files. In addition, there is a possibility to get hashes from the malicious executable files and adding the hashes to the AV's databases in order to detect the malicious files base on the signature-based detection systems.

The proposed design of the new detection system based on the companies' networks is shown in Figure 13.

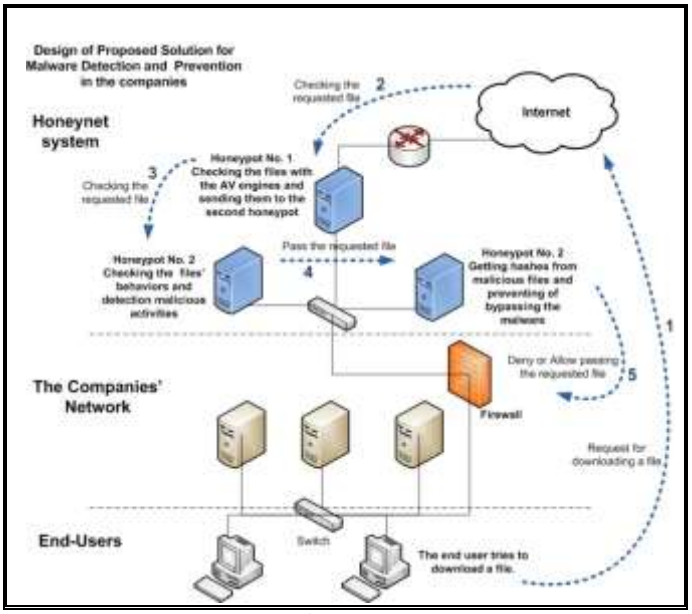

Figure 13: Proposed Solution for Companies Malware Detection and Prevention System.

IV. CONCLUSION AND FUTURE WORK

In terms of penetration testing, many ways such as renamed file extensions, manipulated file headers, compression, embedded, encryption, steganography, out of band attacks, and exploits may use to find the vulnerabilities of an organisation.

There were some methods for bypassing malware defences have been considered. Creating new malware and modifying the malware signature may make the malware to pass the hosed-based AVs. But implementing the honeynet systems for detecting new and unknown malware, increases the rate of detection of the malware. If the victim is protected by a firewall another way such a covert channel over recursive DNS helps the malware to bypass the firewall. To prevent these kinds of attacks, capture the external traffic of the network and using SMTP, HTTP and SSL gateways may helps. Using HTTP gateways to protect the network from malware is quit vulnerable, but adding SSL gateways to them may help to decrease percentage of accessing the malware to the victim.

As it is demonstrated HTTP/SSL gateways has its own weaknesses, for example, if a user gets access to a malicious file over the HTTP/SSL connection and the user download it, the gateway has no chance to detect the malicious file.

Consequently, in future, enhancement of the solution in order to detect the malicious files which are passing over the HTTP/SSL might be considered. In addition, there is possibility to combine the new malware detection and prevention system with green IT technology by utilizing virtualization in the detection system. Implementing virtual honeynet to detect and prevent the unknown malware, brings cost reduction, and it decrease wasting the energy.

REFERENCES

[1] M. Szczepanik and I. Jozwiak, "Detecting New and Unknown Malwares Using Honeynet," *Wroclaw University of Technology, Institute of Informatics, Poland, 2010, p 173.*

[2] R. Richardson. (2008), CSI Computer Crime & Security Survey, Computer Security Institute. Available online at: http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf [Accessed May 2, 2011].

[3] M. Christodorescu and S. Jha, "Testing Malware Detectors," *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis* (ISSTA'04), July 11-14, 2004.

[4] M. Christiansen, Bypassing Malware Defenses," *SANS Institute InfoSec Reading Room*, pp. 3-4 May 7, 2010.

[5] M. Aharoni. (2009, August), Cracking the Perimeter v.1.1, Anti-Virus Comparative No. 23. Available online at http://www.av-comparatives.org/images/stories/test/ondret/avc_report23.pdf [Accessed May 5, 2011].

[6] Panda Security. (2008). Annual Report Pandalabs 2008, Panda Security. Available online at http://pandalabs.pandasecurity.com/blogs/images/PandaLabs/2008/12/31/Annual_Report_Pandalabs_2008_ENG.pdf [Accessed May 2, 2011].

[7] CigiCigi Online. (2010). Turkojan. Available online at http://www.turkojan.com/eng/ [Accessed April 22, 2011].

[8] M. Christiansen, "Bypassing Malware Defenses," *SANS Institute InfoSec Reading Room*, pp. 8-10, May 7, 2010.

[9] Ed. Skoudis, "Security 504: Hacker Techniques, Exploits & Incident Handling," *SANS Institute*, 2006.

[10] L. Zeltser, "Security 601: Reverse-Engineering Malware: The Essentials of Malware Analysis," *SANS Institute*, 2009.

[11] Merriam-Webster Incorporated, 2010. Dictionary and Thesaurus. Available online at http://www.merriam-webster.com/dictionary/steganography [Accessed May 12, 2011].

[12] Honeynet Project Team, "Know Your Enemy: Learning about Security Threats," Second Edition, Addison Wesley Professional Publishers. May 27, 2004.

[13] M. Szczepanik and I. Jozwiak, "Detecting New and Unknown Malwares Using Honeynet," *Wroclaw University of Technology, Institute of Informatics, Poland, 2010, p 173.*

[14] M. Szczepanik and I. Jozwiak, "Detecting New and Unknown Malwares Using Honeynet," *Wroclaw University of Technology, Institute of Informatics, Poland, 2010, p 174-177.*

[15] N.F Huang, Ch.N Kao, G.Y. Jai, Ch.L Lin, " Apply data mining to defense-in-depth network security system," *IEEE International Conference on Advanced Information Networking and Applications (AINA), 2005*, vol. 1, pp. 159-162.

[16] Honeynet Project Team, "Know Your Enemy: Learning about Security Threats," Second Edition, Addison Wesley Professional Publishers. May 27, 2004.