2012

What is the Proper Forensics Approach on Trojan Banking Malware Incidents?

Andri P. Heriyanto
Edith Cowan University, aheriyan@our.ecu.edu.au

DOI: 10.4225/75/57b3ae67fb85f
Originally published in the Proceedings of the 10th Australian Digital Forensics Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

WHAT IS THE PROPER FORENSICS APPROACH ON TROJAN BANKING MALWARE INCIDENTS?

Andri P Heriyanto
School of Computing and Security Science
Edith Cowan University
Perth, Western Australia
aheriyan@our.ecu.edu.au

Abstract

Digital forensics procedures should be developed to obtain digital evidence with regard to legal requirements such as admissibility, authenticity, completeness, reliability and believability. On the other hand, Trojan banking malware incident has grown significantly and creates a great threat to online banking users globally. This type of malware is known to use anti-forensic technique to avoid forensic detection. Moreover, there are numerous works and researches that impose the drawbacks on post-mortem forensics approach in dealing with evidence that only resided on non-persistence memory or non-volatile memory. There are works that reveal the disadvantage of live-response approach on incident response that might compromise the evidence as well. For the last four years, there is notably developed on memory forensics approach that focusing on malware incidents. This paper demonstrates the procedures that use three different forensics approaches on three different Trojan banking malware samples: Cridex, ZeuS and SpyEye. The aim of this work is to obtain the proper forensics approach on Trojan banking malware incidents. The paper also uses a network forensics approach to gather and analyse the network-based evidence.

Keywords
Digital Evidence, Host-Based Evidence, Network Based Evidence, Post-Mortem Forensics, Memory Forensics, Windows Registry Forensics, Trojan banking Malwares

INTRODUCTION

Rowlingson (2004) shows digital evidence is required whenever it can be used to support a legal process. Every digital forensic examiner should consider the legal requirements of digital evidence that consists of admissibility, authenticity, completeness, reliability, and believable (Group, 2002). The examiner is looking at an object that has been designed by people to obtain the digital evidence that might fulfill those requirements when analysing digital data. Furthermore, the storage systems of most digital devices have been designed to be scalable and flexible, and that have a layered design. Carrier (2005) shows the different analysis area with figure below:

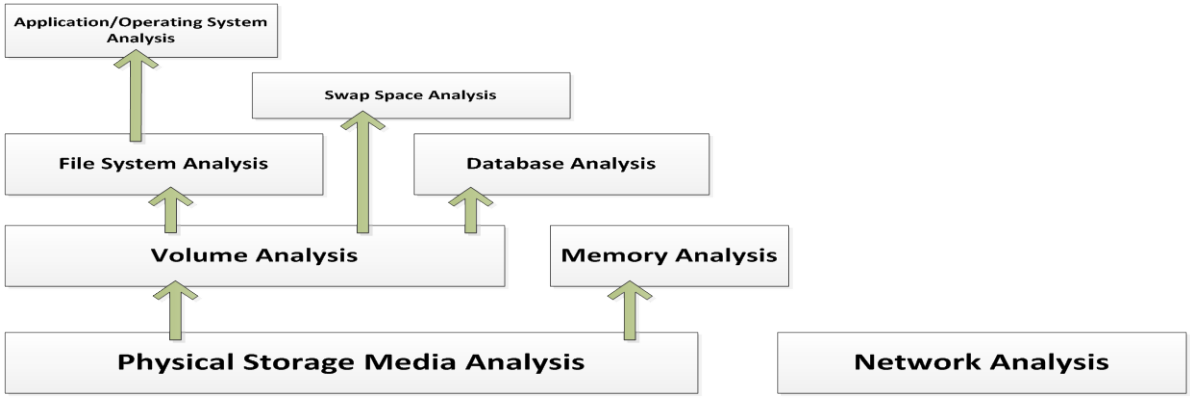

Figure 1: Layers of analysis based on the design of digital data (Carrier, 2005)

This different analysis area creates a multiplicity of subject matter such as computer forensics, database forensics, memory forensics, Windows registry forensics and network forensics. Computer forensics or known as post-mortem forensics involve shutting a computer down to inspect the disks. However, this process breaks network connections and unmounts encrypted disks, resulting in a loss of information and disabling critical processes. Live forensic tools can partially overcome these problems by inspecting active systems (Chan, Chaugule, Larson, & Campbell, 2010). Garcia (2007) reveals that traditional forensic approach, which is, relying in either virtual memory scanning or persistent data, is not sufficient. Subversion techniques such as shadow walker clearly illustrate the need for memory scanners tools aware of malware hiding techniques.

Waits, Akinyele, Nolan, and Rogers (2008) documented three significant setbacks on live response. First, it may rely on Windows API tools. Therefore if the examiner collects the evidence based on compromised sources without they are suspecting it, then this condition could damage the credibility of the evidence in a court of law. Second, the live response is not repeatable and third, the examiners cannot ask new questions later. On the other hand, there is a significantly growing on memory forensics for the last four years. The progress of this field is forced by the need from digital forensic community in dealing with the outgrowth of malicious software such as Trojan banking malwares.

McAfee and Guardian Analytics performed a study on Operation High Roller on 2012 and uncovered a highly sophisticated, global financial services fraud. The study found 60 servers processing thousands of attempted thefts from high-value commercial accounts and some high net worth individuals. Three distinct attack strategies have emerged as the targets have expanded from the European Union, to Latin America, to the United States. Debunking the popular wisdom that only big banks are affected, the research document attacks every class of financial institution: credit union, large global bank, and regional bank. The study estimates the criminals have attempted at least €60 million (US$78 million) in fraudulent transfers from accounts at 60 or more financial institutions (FIs). If all of the attempted fraud campaigns were as successful the total attempted fraud could be as high as €2 billion. Trojan banking malware such as ZeuS and SpyEye might expect to be held liable for those losses (Marcus & Sherstobitoff, 2012).

Brand (2007) reveals that malware can integrate numerous techniques to avoid forensic detection and forensic analysis as well. This technique is known as anti-forensic. Primary goals for anti-forensic is leaving no evidence, avoiding detection, disrupting the collection of information and casting doubt on a forensic report (Garfinkel, 2007). These researches have the same message to digital forensic community: the challenge for collecting the digital evidence in regards with legal consideration.

With the challenge from Trojan banking malwares and the shortcomings on post-mortem forensics and live response, then the question is the proper approach that available for the examiners for collecting the digital evidence on Trojan banking malware incidents. This paper demonstrates how the live response, memory forensic and Windows registry forensics as a representation of post-mortem forensics find the digital evidence on Trojan banking malware incidents. The results will show whether the live response and Windows registry analysis are still the viable options for the examiner on Trojan banking malware incidents. This work also demonstrates network forensics as a conjunction process to obtain more robust and thorough evidence.

This paper uses three different Trojan banking malware samples: Cridex, ZeuS and SpyEye as the object of analysis. The reason for analysing different samples is to acquire the pattern of the malwares and the reason for choosing the malware sample is based on the popularity and the financial impacts on a global scale. This work is far from exhaustive, and serves merely as an introduction to the techniques employed to live response, memory forensics, Windows registry analysis, network forensics and malware analysis of Trojan banking malwares.

This work uses active approach by executing the malware samples on controlled environment. For this paper, legal issue surrounding the behavioural analysis of the malware samples is ignored. It is presumed the malicious software that is being examined is the intellectual property of the organization that will has authorised this activity. Cridex, Zeus and SpyEye as samples on this paper have many different variants. Therefore the results from analysis on this paper works only for the variants that have been used. The different variants from the same malware sample might show a different result.

RELATED WORKS

IOActive (2012) performed a reversal and analysis of the Trojans banking such as SpyEye and ZeuS . The study reveals that SpyEye incorporated many advanced tricks try to hide its presence on the local system. The bot's advanced hooking and injection mechanisms as well as its core functionality used to hijack and steal user information. On the other hand, ZeuS has been identified has additional roadblocks including non-existent import address tables, obfuscated string tables, and relocated code. ZeuS included many methods to hinder reverse engineering.

According to Ståhlberg (2008), the Mstrings approach to Trojan banking analysis and detection seem feasible for the moment. Most current Trojan banking can be detected solely because they include filter strings. Especially if the analysis system has access to the internet, this approach can be used to analyse incoming malware samples. An alert can be sent to targeted banks and this can be done automatically.

On his study of SilentBanker, Theerthagiri (2009) reveals that organizations should think about creating signatures for preventing information leaks and also block all possible sites and IP addresses that host exploits or

drop site of Trojans. Attackers can modify the present code of the Trojan banking and strive to keep their exploit server active. In his study, Dolan-Gavitt (2008) found that it is possible for an attacker with the ability to modify kernel memory to alter the cached registry data in memory, and thus alter the behavior of the operating system, without the changes being visible in the on-disk storage. In the same paper, Dollan-Gavitt also noted that an average of 631 keys and 1231 values per image were volatile and would not have been found using methods that only examine the hives on disk.

Malware researchers show techniques to escape memory analysis using a low-level rootkit (Sparks & Butler, 2005) and that certain virtualization-based rootkits may be hard to detect (Chen & Samuel, 2006). On the other hand, memory forensics researchers show how memory forensics tools such as Volatility could be used for analyzing the Trojan banking malwares for finding the evidence (DiMino, 2012; Malwareninja, 2011).

CHARACTERISTICS OF TROJAN BANKING MALWARES

The detail information of malware samples that have been used on this paper is described on Appendices 1. Additionally, there are six characters of Trojan banking malwares that have been applied as the targets for achieving the objective of this work (OWASP, 2012). Every forensics approach should be worked to find the evidence based on the characteristic. The procedures and tools for acquiring the digital evidence are documented on Appendices 2.

Table 1: Characterization and targets of digital evidence

No	Digital Evidence to Find	Characterization
1	Installation by finding the Worms Copy on the Virtual Machine.	All the Trojan banking malwares are known to have copy of the worms after it was running or execute on the victim's machine. Therefore, the first footprint that indicated the existence of such malware is the worms copy on the victim's machine.
2	Payload (Processes)	After creating the worms copy on the victim's machine, the malware will running its payload through certain services or processes on the victim's machine. There are several researches or works that shows the possibility of such Trojan banking malwares use the anti-forensic techniques to hide its existence or function. The techniques ware used to avoid detection from anti-virus and forensic application, especially on Live Response approach.
3	Network Connections	One of the main purposes of the payload or processes is to create a connection to the Command and Control (C&C) Server.
4	Mutant or Mutex (mutual exclusion) Objects	Malwares often uses mutex objects for the same purpose as legitimate software and to avoid re-infecting the host. Therefore, mutex object is one of persistent signature on the victim's machine.
5	The important information on the particular processes	Trojan banking malwares has documented its target such as particular financial organization, name and IP Addresses of the C&C Server on the particular processes. This information could be obtained by dumping the services and make output strings from it.
6	Firewall Policy	To avoid its existence, the Trojan banking malwares change the firewall policy on the Operating System.

RESULTS

Installation by finding the worms copy on the virtual machine

Live response approach finds the evidence for the installation on the three malware samples. The evidence shows that Cridex has the worm copy with name of the file: **kb00374800.exe.** This worm execution file has found by Autoruns and WinAudit. On Zeus with the name of worm copy: **ntos.exe.** This worm execution file has found by Autoruns, Handle, Rootkit Revealer and WinAudit. On SpyEye with the name of worm copy: **cleansweep.exe.** This worm execution file found by Rootkit Revealer. Memory forensics approach with Volatility finds the existence of worm copy of Cridex on the virtual machine with command: ***printkey -K "Software\Microsoft\Windows\CurrentVersion\Run".*** For Zeus, Volatility finds the existence of worms copy

with command: ***-o 0xe17fea40 -K "Microsoft\Windows NT\CurrentVersion\Winlogon".*** Windows Registry approach with Registry Viewer finds the evidence on Cridex and SpyEye on registry path: ***NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run.*** For Zeus, Registry Viewer finds the existence of worms copy on S***oftware\Microsoft\WindowsNT\CurrentVersion\Winlogon.*** This results show that all approaches could find the evidence of Installation process on the three malware samples.

Payload (Processes)

Live Response approach through Process Explorer records all the suspicious processes on the three malwares samples. Memory Forensic approach also shows the records of all the suspicious processes or payloads on the three malware samples. Windows Registry approach could not deliver the evidence of payloads on the three malware samples.

Network connections

The result for live response approach is documented on the Network-based evidence. Memory forensic approach with Volatility finds several findings: On ZeuS, there is one connection suspected with C&C Server with IP Address 195.2.253.194. This connection was created by the payload (svchost.exe/PID 864). On SpyEye, there is a connection that suspected with C&C Server with IP Address 188.40.138.148. This connection was created by the payload (cleansweep.exe/PID1456). On the Cridex, there is no significant connection that could be identified as a suspicious connection with C&C Server. But according with (DiMino, 2012), his work for analyzing the Cridex shows that there is a connection with the indicated C&C Server. On the other hand, Windows Registry approach could not find the evidence for the connections with C&C Server.

Mutant or mutex (mutual exclusion) objects

There is no mutex objects found by live response approach. Memory Forensic forensics finds 114 mutex objects on Cridex, 125 mutex objects on Zeus and 96 mutex objects on SpyEye. After analyzing all the mutex objects from the three malwares, there are similar 59 mutex object found on all the malwares. It is indicated that those mutex object has been used for avoiding the multiple infections by the three malware samples on the same machine.

The important information on the particular processes

Live response approach could not find the important and relevant strings on the dumping processes. Memory forensics approach could found the important information by dumping the certain processes and create the output strings from it. The suspicious payload (svchost.exe/PID 1164) on Cridex shows the name of DNS that indicated work as a C&C Servers. The suspicious payload (svchost.exe/PID 864) on Zeus shows the IP Address of C&C Servers. The suspicious payload (svchost.exe/PID 1084) on SpyEye shows the name of DNS that indicated work as a C&C Servers. Windows Registry approach could not find the evidence in terms of important information on the registry files.

Firewall policy

Live response approach through WinAudit reports that the Firewall is disabled on Zeus incident. Memory Forensic approach also finds the same evidence that Firewall is disabled by Zeus. The command to find the perimeter of the Firewall Policy on the memory: -K "ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile". Based on the Regshot results, Cridex changes the Firewall Policy on the Registry by opening Port 1900, 2869, 139, 445, 137 and 138. After examining with Registry Viewer on one of File Registry: SYSTEM, then the finding supports the Regshot result. For Zeus, Registry Viewer finds the Firewall Policy on: SYSTEM \CurrentControlSet \Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile with value:”0” (disable).

NETWORK-BASED EVIDENCE

Trojan malwares are highly dependent of the network for propagation, control and payload functionality. Therefore, network forensics is play important role on finding the network-based evidence beside the host-based forensics approach such as post-mortem, live response, and memory analysis. As part of triangulation on obtaining and analyzing the digital evidence, this works documented the network forensics approach on the three malware samples.

Netstat Command

This paper uses comparison of Protocol Connections and TCP/IP network connections on condition before and after running the malware with Netstat command (netstat –ano). TCPView and Port Explorer use in conjunction with the Netstat's comparison to acquire thorough analysis. This comparison and records/log from TCPView and Port Explorer give the summary of the results below:

Table 2: Result of Netstat command, TCPView and Port Explorer

Malware	New Active Connections After Running the Malware	TCPView and Port Explorer
Cridex	Proto Local Address Foreign Address State PID ***UDP 0.0.0.0:64625 *:* 1164***	- There is no record or log on TCPView regarding with the PID 1164 and its relation with TCP/UDP Connections. - The Port Explorer shown the same result with TCPView.
ZeuS	Proto Local Address Foreign Address State PID ***TCP 0.0.0.0:12642 0.0.0.0:0 LISTENING 864*** ***TCP 0.0.0.0:26994 0.0.0.0:0 LISTENING 864*** ***TCP 0.0.0.0:38606 0.0.0.0:0 LISTENING 864***	- There is complete record or log on TCPView regarding with the PID 864 with 3 TCP Connections and its port number. - The Port Explorer shown the same result with TCPView.
SpyEye	Proto Local Address Foreign Address State PID ***UDP 0.0.0.0:55144 *:* 1084***	- There is no record or log on TCPView regarding with the PID 1084 and its relation with TCP/UDP Connections. - The Port Explorer shown the same result with TCPView.

The new active or changing of TCP/IP connection(s) leads to other analysis. The process explorer gives specific information regarding with the specific process/PID. This analysis process is important for finding the payload(s), since Trojan banking malware has known to use API hooking technique to execute its payload. The summary of Process Explorer shown below:

Table 3: Result of Process Explorer

No	Process PID	CPU Private Bytes Working Set Description Company Name	Description
Cridex	*winlogon.exe 624* *svchost.exe 1164*	*6,564 K 356 K Windows NT Logon Application Microsoft Corporation* *1,436 K 88 K Generic Host Process for Win32 Services Microsoft Corporation*	*Parent Process ID*
ZeuS	*winlogon.exe 628* *svchost.exe 864*	*6,804 K 696 K Windows NT Logon Application Microsoft Corporation* *6,832 K 2,116 K Generic Host Process for Win32 Services Microsoft Corporation*	*Parent Process ID*
SpyEye	*winlogon.exe 628* *svchost.exe 1084*	*7,188 K 5,296 K Windows NT Logon Application Microsoft Corporation* *1,640 K 4,104 K Generic Host Process for Win32 Services Microsoft Corporation*	*Parent Process ID*

It reveals that all the malwares install themselves into Winlogon.exe. The purpose is to make sure the payload will be started every time when the Windows OS boots up and from here it will spread to every single process.

Dump the Process and Strings Output

The results from previous analysis could be used as the base of dumping the particular process. Then the analyst could perform an analysis of the Strings Output from it. From the strings output, the analyst might find important and interesting strings which could be used as the evidence. The example of strings output from memory dump of particular process is shown on Appendices 3.

These strings output shows that each malware samples using a different method for stealing the credentials. The strings output from ZeuS reveals the specified IP Address. This information is important for finding the C&C server or who might be responsible for the actions of malware.

Network Packet Capture

Wireshark has been used for examining network traffic for evidence of unusual or malicious traffic on the virtual machine. Using Wireshark to capture traffic to and from a suspect host is an example of reactive analysis (Chappell, 2010).

The network traffics on Cridex and SpyEye show the DNS Protocol packets. This indicates that the payload of Cridex and SpyEye communicates via SSL with a remote server for command and control of the malware. The Cridex was observed to connect with 4 of the following domains for this purpose such as evenconc.ru, extorld.ru, imbingdo.ru and shushev.ru. Almost all the packets or frames were contained with only two protocols: Domain Name Service (DNS) and NetBIOS Name Service. SpyEye was observed creating a connection with horizontalspy.domain.lc with IP Address 188.40.138.148. It is indicating that the domain server works as a C&C Server. Following the TCP Stream for the packets based on the IP Address shows two interesting results:

```
POST http://horizonspy.domain.lc/formgrabber/websitechk.php HTTP/1.1
Host: horizonspy.domain.lc
Connection: close
Content-Type: multipart/form-data; boundary=55377776816118
Content-Length: 667

(skipped)
```

GET
/main/bt_version_checker.php?guid=COMPUTER!VM_TROJAN!18C21DD0&ver=10070&stat=ONLINE&ie=
8.0.6001.18702&os=5.1.2600&ut=Admin&cpu=12&ccrc=0181AD0B HTTP/1.1
User-Agent: Microsoft Internet Explorer
Host: horizonspy.domain.lc
HTTP/1.1 302 Found
Date: Fri, 19 Oct 2012 07:18:15 GMT
Server: Apache/2.2.9
Location:
http://horizonspy.domain.lc/?guid=COMPUTER!VM_TROJAN!18C21DD0&ver=10070&stat=ONLINE&ie=8.
0.6001.18702&os=5.1.2600&ut=Admin&cpu=12&ccrc=0181AD0B

(skipped)

The stream content above is supporting the finding from the strings output from svchost.exe (PID 1084). It is found that the payload create a connection with the C&C Server and perform certain method GET and POST in HTML forms command into the specified URL in order to steal the credential's online banking users.

The packet captures from ZeuS shows interesting results. There is a connection and network packets transferred between virtual machine and IP Address 195.2.253.194 that hosted by spheral.ru. The condition is aligning with the strings output from svchost.exe (PID 864). The strings output documented two specified IP Address: 195.2.253.194 and 64.59.140.93. These IP Addresses were indicated work as the C&C server. Analysis results from Wireshark shows the statistical condition for TCP Endpoints from these connections. There are 17 ports were open to transfer and receive the packets. One port is rootd or port 1094. The rootd daemon works with the TNetFile class. It allows remote access to root database files in either read or read/write mode.

DISCUSSION

The procedures on live-response, memory forensics and Windows Registry approaches for acquiring the digital evidence on the three different Trojan banking malware incidents shows the significant results. Live-response and Windows Registry approaches could find the digital evidence, however there is the possibility of anti-forensics techniques on the malware samples that might compromise the results. All the approaches could identify and obtain the evidence of installation or worm copy on the infected machines. The same result also founds to identify the Firewall Policy that might have been changed by the malwares on the infected machines. On the other hand, memory forensics approach shows the advancement of its technique to find all the target evidence.

Group (2002) reveals every examiner should obtained from the volatile to the less volatile when collecting evidence on incident response. This statement aligned with this work. Almost all the evidence on Trojan banking malware incidents were resided on the physical memory. Therefore, the examiner should avoid performing post-mortem forensics approach on such incidents before they collect and/or analyze the volatile memory.

Walters and Petroni (2007) documented a set of drawbacks on live-response approach when it wants to be used on the incident response. One drawback is live-response might disturbs the state of machine under investigation. This condition is inevitable, since the examiner should run a several Windows API applications to obtain the evidence on the infected machines. Even though the examiner could find the valid and relevant evidence by this technique, but considering the possibility of the disturbance on the victim's machine then it is obvious to use proper forensics approach on Trojan banking malware incidents. If the examiner still insists to perform live response approach, and then it has been advised to perform it after dumping the physical memory.

Network forensics approach shows how to identify the presence of the malware on the network and obtain network-based evidence as a conjunction with host-based evidence. The netstat command as the initial analysis shows the indicated malicious processes or known as payloads. On the other hand, other tools could not detect such processes. On the next process, the examiner could dump the processes and make strings output from it. Moreover, this work shows the importance of the strings. It might contain all relevant and valid information due to the payload functionality and C&C server connections from each malware samples. These finding supports the research by Stahlberg (2007) that most of current Trojan banking could be detected solely based on the filter strings.

CONCLUSION

This paper has demonstrated and discussed the procedures and findings on live-response, memory forensics and Windows Registry forensics approaches. The results might show the proper forensics approach on Trojan banking malware incident for digital forensic examiner with regard to legal requirement on digital evidence. Despite of the approaches, every examiner should prioritize the collection of volatile memory on Trojan banking malware incidents. Memory forensics approach shows the thorough and robust findings with minimal disturbance on the machine. The examiner only needs to dump the physical memory on the first occasion of incidents without running many applications such as Windows API tools on live-response. This approach also offering repeatability and reproducibility factors that might fulfill legal requirement on digital evidence.

This paper also shows the importance of network forensics on Trojan banking malware incidents. Since the Trojan malwares are highly dependent on the network for propagation, control and payload functionality, then examiner might consider collecting the network-based evidence beside the host-based evidence. Both procedures could be performed as a conjunction to acquire more robust and thorough digital evidence. Moreover, the organization could use the network-based evidence such as the strings, suspicious IP Address, and malicious packets to prevent such incidents on the future by adding this information on Intrusion Prevention System/Intrusion Detection System.

REFERENCES

Brand, M. (2007). Forensic Analysis Avoidance Techniques of Malware.

Carrier, B. (2005). *File system forensic analysis*: Addison-Wesley Professional.

Chan, E., Chaugule, A., Larson, K., & Campbell, R. (2010). *Performing Live Forensics on Insider Attacks.* Paper presented at the 2010 CAE Workshop on Insider Threat.

Chappell, L. A. (2010). *Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide*: Protocol Analysis Institute, Chappell University.

Chen, P., & Samuel, K. (2006). *SubVirt: Implementing malware with virtual machines*.

DiMino, A. M. (2012). Cridex Analysis using Volatility, from http://sempersecurus.blogspot.com.au/2012/08/cridex-analysis-using-volatility.html

Dolan-Gavitt, B. (2008). Forensic analysis of the Windows registry in memory. *digital investigation, 5*, S26-S32.

Garcia, G. L. (2007). Forensic physical memory analysis: an overview of tools and techniques. *Helsinki University of Technology, October*.

Garfinkel, S. (2007). *Anti-forensics: Techniques, detection and countermeasures.* Paper presented at the The 2nd International Conference on i-Warfare and Security (ICIW).

Group, T. I. S. N. W. (2002). Guidelines for Evidence Collection and Archiving *RFC 3227*.

IOActive, I. (2012). Reversal and Analysis of Zeus and SpyEye Banking Trojans.

Malwareninja. (2011). Zeus Analysis in Volatility 2.0, from https://malwarereversing.wordpress.com/2011/09/23/zeus-analysis-in-volatility-2-0/

Marcus, D., & Sherstobitoff, R. (2012). Dissecting Operation High Roller: McAfee and Guardian Analytics.

OWASP. (2012). OWASP Anti-Malware-Knowledge-Base, 2012, from https://www.owasp.org/index.php/OWASP_Anti-Malware_-_Knowledge_Base#Cridex

Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence, 2*(3).

Sparks, S., & Butler, J. (2005). Shadow Walker": Raising the bar for rootkit detection. *Black Hat Japan*, 504-533.

Ståhlberg, M. (2008). *The trojan money spinner*.

Theerthagiri, D. (2009). Reversing Malware: A detection intelligence with in-depth security analysis.

Waits, C., Akinyele, J. A., Nolan, R., & Rogers, L. (2008). Computer Forensics: Results of Live Response Inquiry vs. Memory Image Analysis: Software Engineering Institute Carnegie Mellon University

Walters, A., & Petroni, N. (2007). Volatools: integrating volatile memory forensics into the digital investigation process. *Black Hat DC, 2007*.

APPENDICES

Appendices 1: Detail information and source of malware samples

Table 4: Detail information and source of malware samples

No	Malware Sample	Source
1	**Cridex Trojan Banking** MD5: e92de5cc06a361575d24adbde4bf0e81 SHA1: 29fc820e7e989f961cf7eab24a4f553488a60307	http://oc.gtisc.gatech.edu:8080/search.cgi?search=cridex
2	**ZeuS Trojan Banking** MD5: fb4d991644686160625eafe0c589392b SHA1: 944810e76932d83e338d25711175fc66903c8c0a	http://oc.gtisc.gatech.edu:8080/search.cgi?search=zeus
3	**SpyEye Trojan Banking** MD5: 79ac48be8de57d54764fdd22c0fe3f16 SHA1: 38f0f5d3849e78a1e0fb6f83e9fedf8f45d1cffb	http://oc.gtisc.gatech.edu:8080/search.cgi?search=spyeye

Appendices 2: Tools and Procedures

Table 5: Tools and procedures on live response approach

o	Tools	Procedures
1	Running several applications: a. Process Explorer v15.23, b. Autoruns for Windows v11.34, c. Handle v3.5	Autoruns 1. Autoruns Options: - Hide Microsoft and Windows Entries; - Verify code signatures. 2. Save the output scan for comparison process. Process Explorer: 1. Paused by pressing the space bar Handle: Run and save the result
2	*Running the Malware*	
3	a. Handle v.3.5 b. Autoruns; c. Process Explorer.	1) Run Handle and save the result. 2) Refresh Autoruns and Process Explorer.
4	a. Autoruns; b. Process Explorer's	1) Run compare function on Autoruns and save the result; 2) Check the suspicious program on Autoruns for its processes on Process Explorer; 3) Save the Process Explorer's capturing process; 4) Check for any suspicious highlighted process on Process Explorer and records/save the results. 5) Check the digital signature with Process Explorer for any suspicious processes and records/save the results; 6) Dump the suspicious processes and save the strings with Process Explorer.
5	- VMMap	1) Run the VMMap against the suspicious processes 2) Use VMMap's strings dialog for any suspicious processes. 3) Save the results;
6	WinAudit Freeware v.2.29	Run WinAudit and save the result.
7	RootkitRevealer v1.71	Scan for any presence of the rootkit on virtual machine.
8	Analysis	Analyse all the results from the tools above.

Table 6: Tools and procedures on memory forensics approach

No	Tools	Procedures
1	VMware Player with Windows XP SP3x86 as the Operating System	Suspend the virtual machine and copy the vmem for analysis process.
2	Volatility ver. 2.2	Analyse with Volatility ver. 2.2

Table 7: Tools and procedures on windows registry forensics approach

No	Tools	Procedures
1	VMware Player with Windows XP SP3x86 as the Operating System	Shutdown and booting the virtual machine
2	FTK Imager	Acquire the Windows Registry with FTK Imager
3	Registry Viewer	Analyse the Windows Registry with Registry Viewer

Table 8: Tools and procedures on network forensics approach

No	Tools	Procedures

1	Running several applications: a) Regshot v.1.8.3; b) TCPView v.2.54 c) Port Explorer d) Wireshark both on Guest and Host e) Netstat on Operating System;	Regshot: Capture 1st conditions Netstat-ano: Run Netstat –ano from command prompt and Save on notepad. Wireshark: Capture the packet
2	*Running the Malware*	
3	f) Wireshark g) Netstat **h)** Regshot:	a) Wireshark: capture the packet; b) Run Netstat –ano from command prompt and save on notepad. c. Reghsot: capture 2nd condition and run compare function and save the result;
4	Analysis	Analyse all the results from the tools above.

Appendices 3: Example of Strings Output Results

TABLE 9: EXAMPLE OF STRINGS OUTPUT RESULTS

Malwares	Example Strings Output
Cridex	svchost.exe.2486c10.0x00630000-0x0066ffff.dmp: shushev.ru svchost.exe.2486c10.0x00630000-0x0066ffff.dmp: shushev.ru.localdomain svchost.exe.2486c10.0x76770000-0x7677cfff.dmp: Logging information for DNS Caching Resolver service svchost.exe.2486c10.0x76770000-0x7677cfff.dmp: System Time Information svchost.exe.2486c10.0x76770000-0x7677cfff.dmp: DNS Caching Resolver service svchost.exe.2486c10.0x76770000-0x7677cfff.dmp: d:\nt\ds\dns\resolver\server\remote.c svchost.exe.2486c10.0x76770000-0x7677cfff.dmp: d:\nt\ds\dns\resolver\server\rpc.c svchost.exe.2486c10.0x76f20000-0x76f46fff.dmp: www.microsoft.com svchost.exe.2486c10.0x76f20000-0x76f46fff.dmp: microsoft.com svchost.exe.2486c10.0x76f20000-0x76f46fff.dmp: update.microsoft.com svchost.exe.2486c10.0x76f20000-0x76f46fff.dmp: download.microsoft.com svchost.exe.2486c10.0x76f20000-0x76f46fff.dmp: microsoftupdate.com svchost.exe.2486c10.0x76f20000-0x76f46fff.dmp: windowsupdate.com
ZeuS	svchost.exe.23d7da0.0x00090000-0x0018ffff.dmp: Ahttps://onlineeast#.bankofamerica.com/cgi-bin/ias/*/GotoWelcome svchost.exe.23d7da0.0x00090000-0x0018ffff.dmp: Password: %s svchost.exe.23d7da0.0x00090000-0x0018ffff.dmp: Type: %s svchost.exe.23d7da0.0x00090000-0x0018ffff.dmp: Version: %S svchost.exe.23d7da0.0x00090000-0x0018ffff.dmp: Balance: svchost.exe.23d7da0.0x00090000-0x0018ffff.dmp: C:\WINDOWS\system32\config\systemprofile\Local Settings\Temporary Internet Files\Content.IE5\ svchost.exe.23d7da0.0x00090000-0x0018ffff.dmp: Ahttps://www.e-gold.com/sci_asp/payments.asp svchost.exe.23d7da0.0x00090000-0x0018ffff.dmp: A*PAYMENT_AMOUNT= svchost.exe.23d7da0.0x00090000-0x0018ffff.dmp: APAYEE_ACCOUNT=*& svchost.exe.23d7da0.0x00090000-0x0018ffff.dmp: APAYEE_ACCOUNT=%u& svchost.exe.23d7da0.0x00090000-0x0018ffff.dmp: Application/x-internet-signup svchost.exe.23d7da0.0x00090000-0x0018ffff.dmp: ://195.2.253.194/lsd/tt.bin svchost.exe.23d7da0.0x00090000-0x0018ffff.dmp: /lsd/tt.bin HTTP/1.1 svchost.exe.23d7da0.0x00090000-0x0018ffff.dmp: ://195.2.253.194/lsd/tt.bin

	svchost.exe.23d7da0.0x00090000-0x0018ffff.dmp: http://64.59.140.93/wpad.dat
SpyEye	svchost.exe.2225ca8.0x00090000-0x0018ffff.dmp: ost.exe svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: _AVIRA_ svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: __SYSTEM__ svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: *call*event* svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: call_event svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: onclick svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: target svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: American Express svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: Visa svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: MasterCard svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: Discover svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: Smth wrong with navigate to BILLING-PAGE. 0_o svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: *We are sending* svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: *Thank You For Your Order* svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: core-section-header svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: confirm:card_exp_year svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: Cannot find Month stuff on second page. 0_o svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: confirm:card_exp_month svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: Cannot find CSC stuff on second page. 0_o svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: confirm:card_security_code svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: Cannot find CardNumber stuff on second page. 0_o svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: confirm:card_number svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: http://www.microsoft.com svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: horizonspy.domain.lc svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: http://horizonspy.domain.lc/formgrabber/websitechk.php svchost.exe.2225ca8.0x0ea50000-0x0ea78fff.dmp: http://horizonspy.domain.lc/formgrabber/websitecheck.php