SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Jurnal & Penelitian Teknik Informatika
Volume 3 Nomor 1, April 2018
e-ISSN : 2541-2019
p-ISSN : 2541-044X

# Reverse Engineering Analysis Forensic Malware WEBC2-DIV

[1st]Raditya Faisal Waliulu
Department of Informatics Egineering
Universitas Muhammadiyah Sorong
Sorong, Indonesia
raditya@um-sorong.ac.id

[2nd]Teguh Hidayat Iskandar Alam
Department of Informatics Egineering
Universitas Muhammadiyah Sorong
Sorong, Indonesia
teguhhidayat@gmail.com

***Abstract*** – At this paper focus on Malicous Software also known as Malware APT1 (Advance Presistent Threat) codename WEBC2-DIV the most variants malware has criteria consists of Virus, Worm, Trojan, Adware, Spyware, Backdoor either Rootkit. Although, malware could avoidance scanning antivirus but reverse engineering could be know how dangerous malware infect computer client. Lately, malware attack as a form espionage (cyberwar) one of the most topic on security internet, because of has massive impact. Forensic malware becomes indicator sucessfull user to relized about malware infect. This research about reverse engineering. A few steps there are scanning, suspected packet in network and analysis of malware behavior and dissambler body malware.

***Keyword – forensic malware, Analysis, Advance Presistent Threat, Cyberwar, disassembler, static analysis, dynamic analysis***

## I. INTRODUCTION

Recently a number of program created for criminal and illegal purpose growth fast. This Program is malware that creates a growing organization, a criminal computer. Definitely, criminal malware take over client's computer and steal personal data, confidential or information of a beneficial nature. this case presure investigation digital forensic and research security to secure malware attack analysis and use tools that can be relied on beside antivirus.

Today, malware forensics take a part [4]. The aim malware forensic that can identified and analyzed malware which undefined. Many malware created has capable to avoid detection antivirus. Because of that, needs to know analyz malware should be detail about malware capability it self until known impact damage and theft personal data.

Privacy safety, integrity and availability in a real computer system is a challenging task. Increasing amount of system and complex malware between both of them makes secure protection and accurate every system could take time and prone to error.

Thanks to Ministry of Research, Technology and Higher Education for grant lecturer beginner research . The beginner lecturer research grant is hopeful that it will continue to automate malware detection cutting down scan time.

A discussion of the fundamental challenges and issues/characteristics of malware has been done. Identification of security and privacy issues within this framework are highlighted . Study of the widely used encryption techniques by malware damage in securing sensitive information on cloud is debated. Scope has been set for academicians and researchers. Diverse versions of the encryption techniques surveyed and analyzed to identify harmfull or damage for cloud security [11].

## II. LITERATUR REVIEW

Malware analysis must be detailed and it take a long time. Malware avoid faced antivirus categorized good one. But, any aspect malware hide from antivirus and it's hard to detected. A few malware forensic tools can show value hidden malware is. In addition, forensic techniques on various tools and plugins more than avoidance analysis techniques. This has become one of the bases for software investigated [3].

Malware analysis one of security computer analyzed malware, learn how and malware's behave. Malware analysis has two method statis analysis and dynamic analysis. Analysis statis is method dissamble malware without running. But, dynamic analysis is running malware and look for behave itself [18] Framework or pattern recognition techniques are applied for detection of packed malware binaries. The

proposed divided in two phases, first phase it classified packed and non-packed executables. Once an executable is classified as packed, the second phase of classification finds packed benign or packed malware executable. Result framework gain more than 99.9% accuracy in the first phase of classification and 95% accuracy in the second phase of classification [5].

High demand Internet data transfer needs is highly dependent on social factors. because the development of technology is increasingly encouraged to understand the mobility of end user needs. not limited only that Human Resources must also be encouraged to know more about the latest technology updates [14].

At this paper focus on malware forensic, a few malware has typical one of virus, trojan, adware, spyware, backdoor, and rootkit capable attack fast to infect operating system [6].

## III. TAXONOMY OF MALICIOUS SOFTWARE

Created malicious software high growth for cyberwar and spionage there are computer virus which might be confused, such as backdoor, worm and etc [5]. According that following paragraphs offer definitions of these types of malicious software and explanations:

### A. Malware

Contraction of malicious software. Put simply, malware is any piece of software that was written with the intent of doing harm to data, devices or to people. Theses family of malware, including worms, viruses, Trojan horses, backdoors, bombs and rootkits.

### B. A Trojan horse

a program that appears to be legal and executed by victim that gives the attacker unauthorised remote access to a system it can be harmful or advantages by attacker.

### C. A virus

Recursive code it can replicates itself. In other words, virus could attach in processes or be harm on computer.

### D. A worm

Infect computer needs skill social engineering, does not host or human to propagate. Worm works on file-transport or information-transport features on the system, allowing it to travel unaided.

### E. Rootkits

Special tools used to attacker that allows someone to takeover a computer without the computer user/owner knowing about.

### F. A backdoor

After take over computer victim's by bypass defense system operating. in could gain unauthorised access and remote.

## IV. ANALYSIS

At this section we describe our proposed malware analysis schema reasearch forensic malware host and guest Windows XP SP3. Phicys host IP 192.168.56.1 and Guest IP 192.168.56.101 this we use bridge interface, fig 1

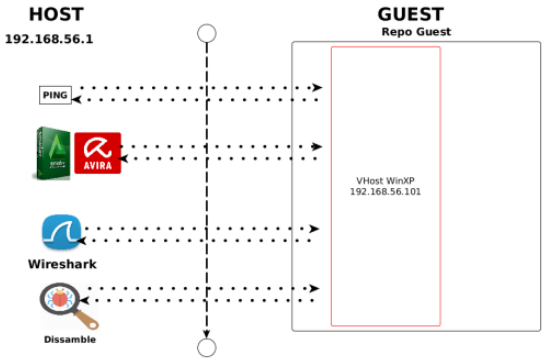


Figure 1 Porposed Model Forensic

Analysis malware, there are two main techniques for analysis malware that are the most commonly used method was static analysis and dynamic analysis. Static analysis is a method of analysis of malware that done without running the malware, so analysis using this method is much more secure than using the method of dynamic analysis. fig 2

e-ISSN : 2541-2019
p-ISSN : 2541-044X

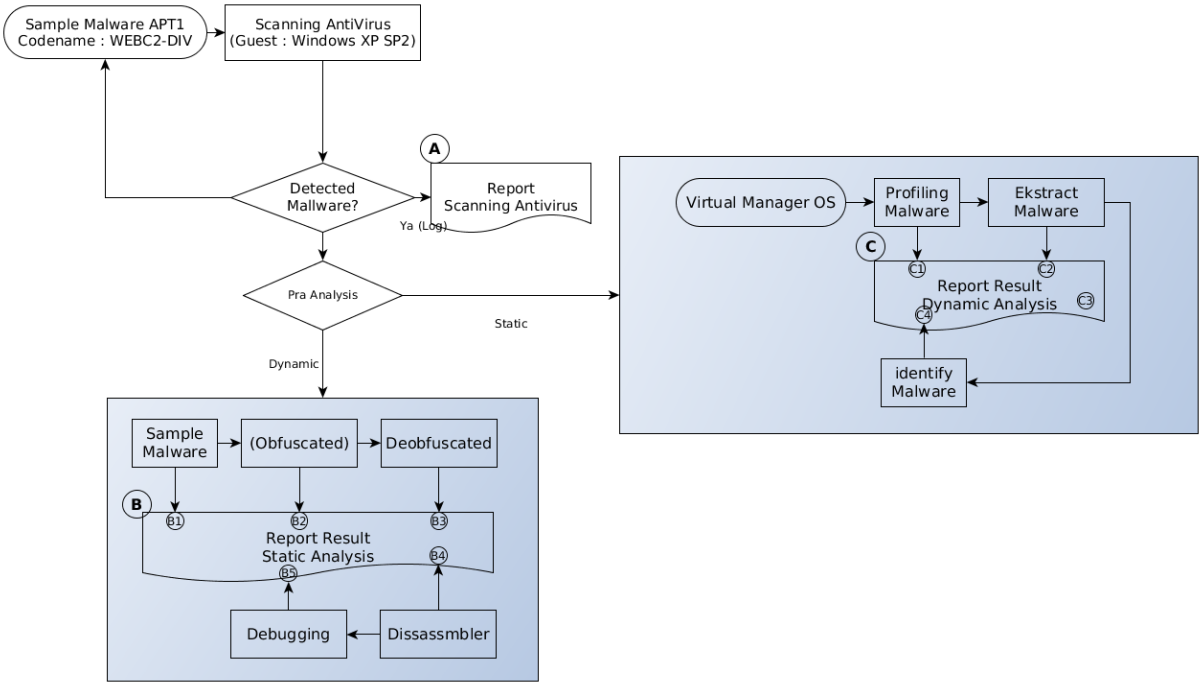


Figure 2 Anaylsis Malware

Malware WEBC2-DIV running at Guest, at Figure line blue malware running in name Div.exe, fig 3

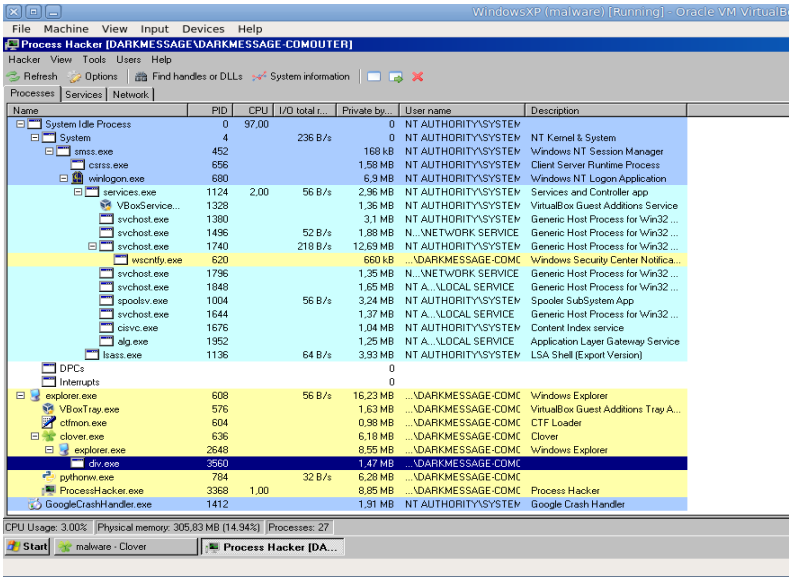


Figure 3 Process Hacker determine WEBC2-DIV

After div.exe running at guest, wireshark on host trying to suspect through network, string cleartext we get and malware trying to connect to thecrowngolf.org, fig 4

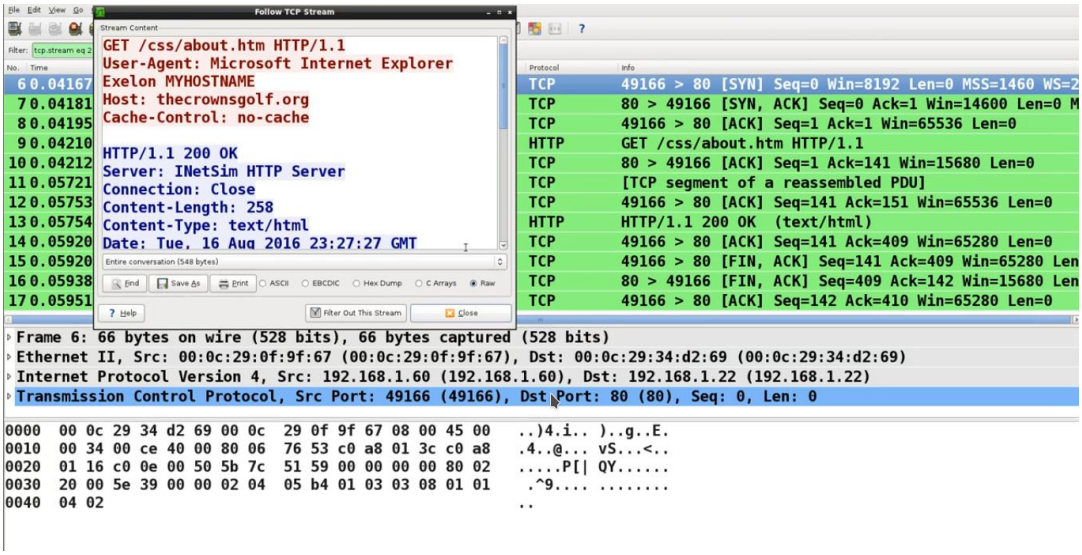


Figure 4 Host Excute Wireshark

Step before doing reverse engineering, host to do dissambler at OS Parrot OS and Kernel 3.16-04, fig 5.

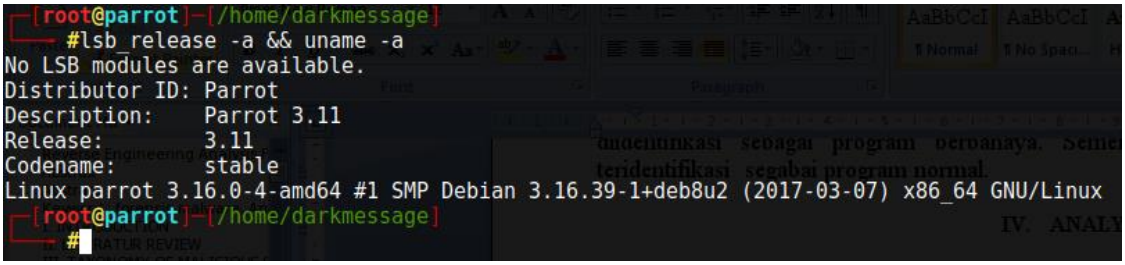


Figure 5 Host Disassembler

First of all overview about file div.exe malware using Cutter software. Running cutter and insert div.exe we get information about Hash and Library, at fig 6

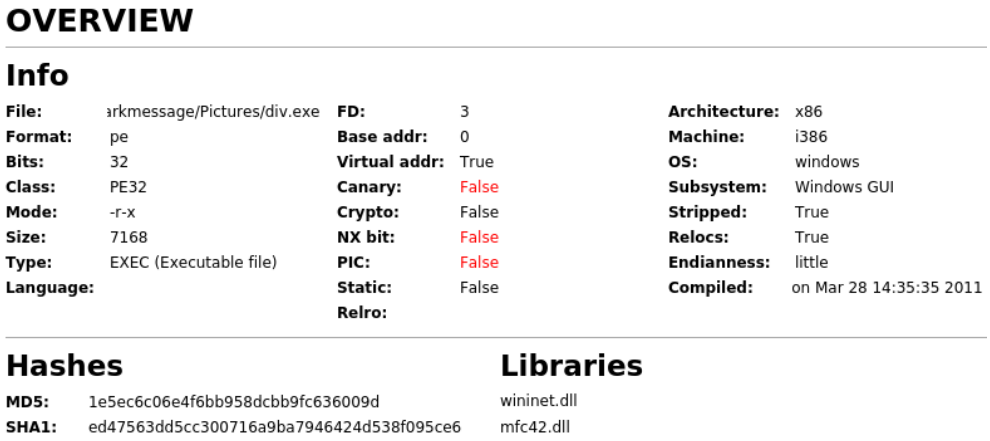


Figure 6 Overview Malware WEBC2-DIV

It's time to do dissamble on the malware body so it is found that the behavior of the parent malware on the guest and do the planting value in regedit windows address

HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Run. Can be seen in color blocks like fig 7

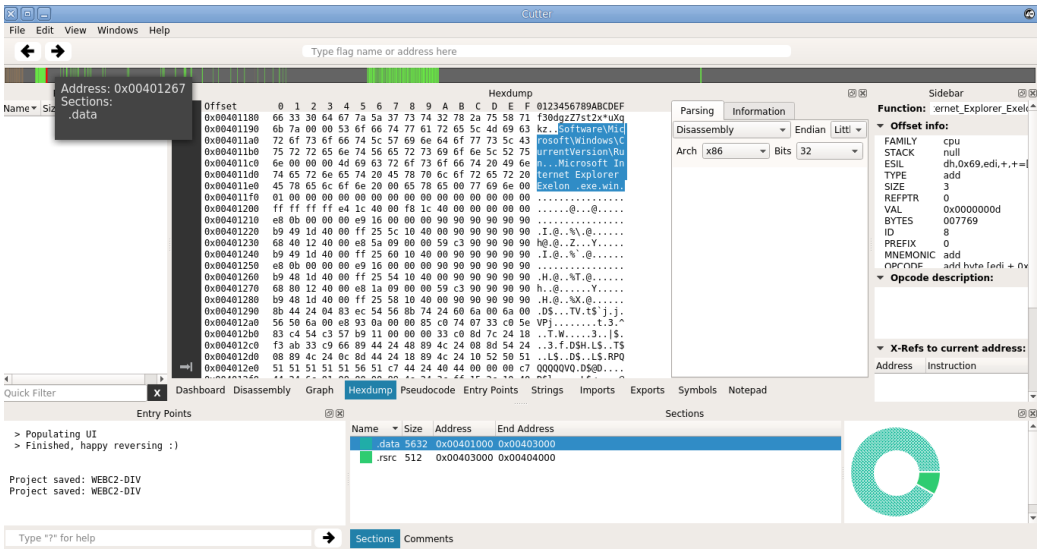


Figure 7 Address Malware On Regedit Windows

State disassemble not stop at this, body malware got encryption that held important message can infected security computer then could be harmful. Like the encryption block color as fig 8 and fig 9

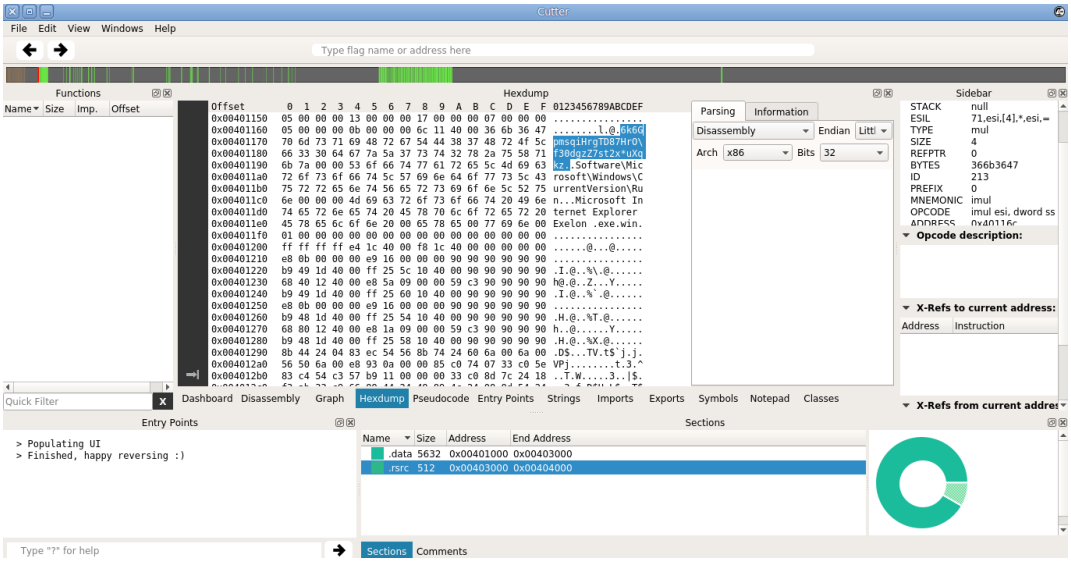


Figure 8 HexDump value encrypt malware WEBC2-DIV

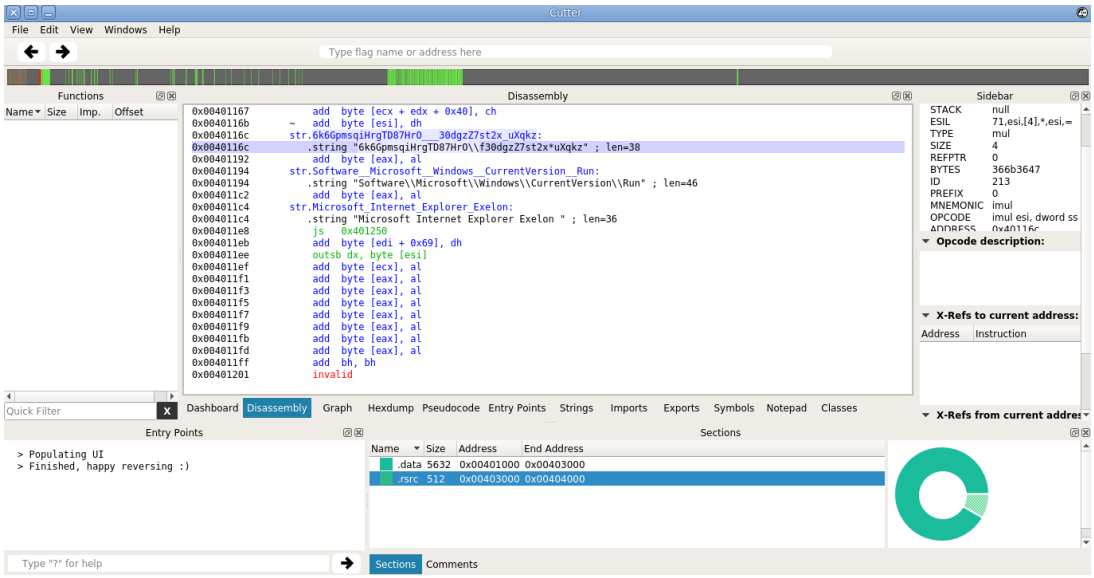


Figure 9 Value string WEBC2-DIV encrypt on disassembler

Decode encrypt to get information about malware's behave. One another hand, details where's malware sent data to his creator. Result decode we get as fig 10.

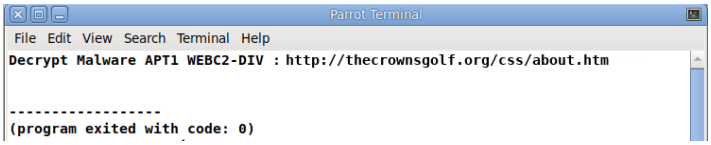


Figure 10 Decode String Encrypt

## V. CONCLUSION

After all doing reverse engineering, WEBC2-DIV encode body's malware as secure as to take over user pc as espionage and mount dns on thecrownsgolf.org. hard to decode because string use different algorithm encrypt.

Then, malicious embedded itself on regedit, explorer.exe and body. There is not clone itself but the developer WEBC2-DIV makes to hard remove them from PC victims.

WEBC2-DIV used to espionage activities performed there are : (1) Phising email, (2) Phising login credential, (3) Backdoor, (4) Remote trojan. This malware well-known since 2010. That does not out posibility malware WEBC2-DIV do update itself by creator then encryption in body malware more difficult than before.

At last word, this research aims to tell careful about what we download and installed on computer or laptop. Many programs created to have special infected and record anything if victim connected to internet.

## REFRENCES

[1] Ahmed.F.S., J. A.-C. (2012). Towards Automated Malware Behavioral Analysis and Profiling for Digital Forensic Investigation Purposes. *4th International Conference on Digital Forensics and Cyber Crime ICDF2C 2012.* Lafayette, Indiana, USA.

[2] Armbrust, M. F. (2010). A view of cloud computing. *Communications of the ACM*, (pp. pp 50-58).

[3] Brand, M. V. (2010). Malware Forensics: Discovery of the Intent of Deception. *Journal of Digital Forensics, Security and Law , Vol 5* (4), 31 - 42.

[4] Daoud, E. A. (2 September 2008). Vol 1. No.2 Computer Virus Stategies and Detection Methods. In *Int. J. Open Probles Compt. Math.*

[5] Davis, M., Bodmer, S., & Lemasters, A. (2010). In *Hacking Exposed Malware and Rootkits.* McGraw-Hill, Inc.

[6] Devi, D. d. (2012). Detection of Packed Malware. *Proceeding SecurIT '12 Proceedings of the First International Conference on Security of Internet of Things* (pp. 22 - 26). NY: ACM.

[7] Distler, D. (2007). Malware Analysis : An Introduction. *Journal Of SANS Institute* .

[8] Jeong K, H. a. (2008). Code graph for malware detection, in:Information Networking. *ICOIN (International Conference)* , 1-5.

[9] Juels, A. d. (2013). New Approached to Security and Availabilitu to Cloud COmpuing. *AC<-RSA Lboratories* .

[10] Kim, K. d.-R. (2010). Malware detection based on dependency graph. *in: Proceedings of the 12th annual conference on Genetic and evolutionary computation* (pp. 12-18). NY, USA: ACM.

[11] Mahboob, T. Z. (2016). Adopting Information Security Techniques for Cloud Computing–A Survey. *International Conference on Information Technology*, (pp. pp 7 - 11). Yogyakarta: Information Systems and Electrical Engineering (ICITISEE).

[12] Mariana, C. M. (2011). Secure Computing Benefits, Risk and Controls. *IEEE-Information Security* , Soutch Africa.

[13] Mell, P. d. (2011). *The NIST definition of cloud.* U.S: National Institute of Standards and Technology.

[14] Raditya, W. F. (2013). RANCANG BANGUN APLIKASI UNTUK MENYERANG BALIK DARI PENGGUNA NETCUT DIJARINGAN LOCAL DENGAN MENGGUNAKAN DDOS. *Skripsi, Fakultas Ilmu Komputer.*

[15] Shang, S. Z. (October 19–20, 2010). Detecting malware variants via function-call graph similarity. *in: 5th International Conference on Malicious and Unwanted* (pp. 113-120). Nancy, France: IEEE.

[16] Sharif, M. Y. (2008). In *Eureka: A Framework for Enabling Static Malware Analysis* (pp. 481-500). Berlin, Heidelberg: Springer.

[17] Sikroski., M. H. (2012). *Practical Malware Analysis.* San Fransisco.

[18] Syarif, S. Y. (2015). Implementation of Malware Analysis using Static and Dynamic Analysis Method. *International Journal of Computer Applications , 117* (6), 11 - 15.

[19] Vigna, G. (2014). *Antivirus isn't Dead, It Just Can;t Keep Up.* Lastline Labs.