Reverse Engineering Analysis Statis Forensic Malware Webc2-Div

Raditya Faisal Waliulu[a*], Teguh Hidayat Iskandar Alam[b*]

[ab] Fakultas Teknik, Program Studi Teknik Informatika, Universitas Muhammadiyah Sorong

Abstract

At this paper focus on Malicious Software also known as Malware APT1 (Advance Persistent 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 successful user to realized about malware infect. This research about reverse engineering. A few steps there are scanning, suspected packet in network and analysis of malware behavior and disassembler body malware.

Keyword : forensic malware, analysis, advance persistent threat, cyberwar, disassemble, static analysis, dynamic analysis

Abstrak

Pada paper ini terfokus pada *malicious software* atau malware APT1 (Advance Presistent Threat) dengan code name WEBC2-DIV yang menjadi salah satu varian malware yang mewakili sifat dari Virus, Worm, Trojan, Adware, Spyware Backdoor Ataupun Rootkit. Meski malware dapat menghindari scanning antivirus namun dengan teknik reverse engineering dapat dilakukan meski menyita waktu karena dengan teknik ini dapat mengetahui seberapa bahaya malware yang menginfeksi. Penyerangan menggunakan malware hacker menjadi trend espionage dari sebuah negara (cyberwar), karena memiliki dampak begitu besar dari sisi materil dan non materil. *forensic* malware menjadi tolak ukur keberhasilan bahwa setiap pengguna Komputer akan sadar bahaya malware. Pada penelitian ini terfokus pada reverse engineering malware. Beberapa langkah analisis diantaranya berawal dari pindai aplikasi yang menyerupai malware, mencurigai paket yang bergerak pada jaringan, analisis tingkah laku malware.

Kata kunci : forensic malware, Analysis, Advance Presistent Threat, Cyberwar, dissambler

1. Pendahuluan

Baru-baru saja, angka program dibuat untuk tujuan kriminal dan ilegal bergerak cepat. Program ini adalah malware yang diciptakan mendukung pertumbuhan organisasi, kriminal komputer. Tentu saja, keuntungan kriminal malware mengambil alih komputer dan mencuri personal data, confidential atau informasi yang bersifat menguntungkan. Angka kriminal malware bergerak cepat memaksa Digital Forensik Investigasi dan riset kemananan untuk melakukan malware analisis dan menggunakan *tool* lainnya yang mampu diandalkan selain antivirus.

Saat ini, Malware Forensics telah menjadi bagian komputer forensics (Daoud, 2 September 2008). Tujuan dari Malware Forensics ini adalah mengidentifikasi dan menganalisis malware yang tidak dikenal. Banyak malware yang ciptakan dengan kemampuan menghindari deteksi antivirus. Oleh karena itu, perlu diketahui analisi malware lengkap mengenai kemampuan malware sehingga mampu mengetahui dampak kerusakkan hingga pencurian data yang dilakukan oleh malware.

Perlindungan kerahasiaan, integritas dan ketersediaan dalam sistem komputer sesungguhnya adalah tugas yang menantang. Meningkatnya jumlah objek sistem dan interaksi kompleks malware di antara keduanya membuat perlindungan yang aman dan akurat dari setiap objek sistem yang memakan waktu dan rawan kesalahan.

Komputasi banyak digunakan sebagai penyimpanan data on-demand namun melibatkan banyak resiko seperti keamanan, perlindungan privasi, akses kontrol dan kerahasiaan data. Peniliti saat ini mengumpulkan informasi survey teknik *malware forensics* berguna untuk mengamankan informasi sensitif. Identifikasi masalah keamanan dan privasi pada mallware hal ini yang di sorot. Studi teknik *malware forensics* memantu mengamankan sensitif informasi hingga saat ini diperdebatkan. Lingkup telah ditetapkan untuk akademis dan peneliti. Berbagai teknik forensik dilakukan pada survey dan analissa untuk identifikasi fitur pengoptimalan untuk keamanan (Mahboob, 2016).

2. Kerangka Teori

Analisis Malware harus secara rinci dan sungguh sangat menyita waktu. Teknik Analisis penghindaran malware terhadap AntiVirus dapat di golongkan sangat bagus. Namun, ada Kecendrungan alat analisis terfokus pada malware yang bersembunyi dari pada mendeteksi malware tersebut, dan bukan menjadi alat pendeteksi dan mencatat teknik penghindaran analisis. Selain itu, cakupan teknik anti-anti analisis pada berbagai tool dan plugin jauh lebih sedikit dari pada angka teknik analisis penghindaran. Hal ini menjadi salah satu dasar untuk perangkat lunak diselidiki [3].

Malware analisis merupakan cabang ilmu keamanan komputer menganalisis malware dan bagaimana memperlajari komponen dan prilaku malware. Analisis malware menggunakan dua metode analisis statis dan analisis dinamis. Analisis statis adalah metode yang dilakukan tanpa menjalankan malware. Sedangkan Analisis dinamis adalah metode forensik yang dilakukan dengan menjalankan program malware [18].

Penerapan teknik pengenalan paket deteksi biner malware. Objek yang didapatkan diambil ciri khasnya dari dari hasil decode *.exe file kemudian dikelompokkan. Pengelompokkan dibuat menjadi 2 fase, fase pertama pengelompokkan file *.exe atau file type malware. fase kedua pengelompokkan tersebut di pisahkan menjadi malware jinak atau malware executeable. Lingkup kerja pada UPX packer backdoord dan Rootkit mampu menyerang cepat menginfeksi Sistem Operasi Microsoft Windows (Distler, 2007).

3. Aturan Struktur Malicious Software

Malicous software semakin pesat diciptakan untuk melakukan cyberwar pada era digital. Perkembangan ini tidak menutup kemungkinan tercipta sebagai varian baru atau kemutakhiran. Disusun berdasarkan hirarki sebagai berikut :

3.1 Malware

Frase dari malicious software. Di definisikan program komputer yang mencoba membahayakan sistem komputer dari client yang tidak mengerti mengenai sebuah sistem komputer. Ada beberapa kategori malware termasuk worm, viruses, Trojan horse, backdoors, bombs, rootkits.

3.2 Trojan horse

Program yang muncul awal kalinya legal dan di eksekusi jarak jauh dari sipembuat untuk menyerang sistem komputer secara unauthorised remote access.

3.3 Virus

Code recursively menduplikasikan dirinya sendiri. Dengan kata lain, program komputer yang menempel pada file atau proses lain.

3.4 Worm

Sebuah program yang dirancang untuk menginfeksi komputer host dengan mereplikasi dirinya sendiri di seluruh jaringan.

3.5 Rootkits

Spesial tools yang digunakan penyerang setelah membobol sistem komputer, untuk mendapatkan hak akses penuh mendapatkan hasil analisa yang mencapai 99.9% akurat pada fase pertama pengelompokkan dan mencapai 95% akurat pada fase kedua (Devi, 2012).

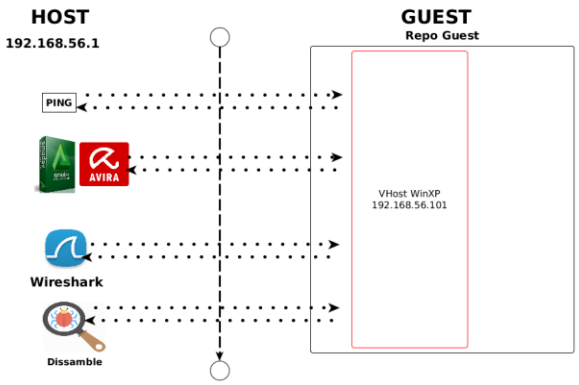
Tingkat kebutuhan dan cepatnya transfer data internet sangat tergantung oleh faktor lingkungan dan sosial. karena perkembangan teknologi semakin terpacu untuk memahami mobilitas kebutuhan end user. tidak terbatas hanya itu saja SDM pula harus terpacu untuk mengetahui lebih tentang update-an teknologi terkini (Raditya, 2013).

Penelitian mengenai Malware Analisis menerapkan metode analisis statis (code) dan analisis dinamis (behavioral), digambarkan berbagai tipe malware diantaranya mewakili Virus, Trojans, Adware, Spyware,

Identifikasi ini tidak selamanya akurat, kineja sistem keamanan komputer seharusnya mempertimbangkan alarm false positif dan false negative. False positif terjadi ketika program normal diidentifikasi sebagai program berbahaya. Sementara, False negative adalah program jahat teridentifikasi segabai program normal.

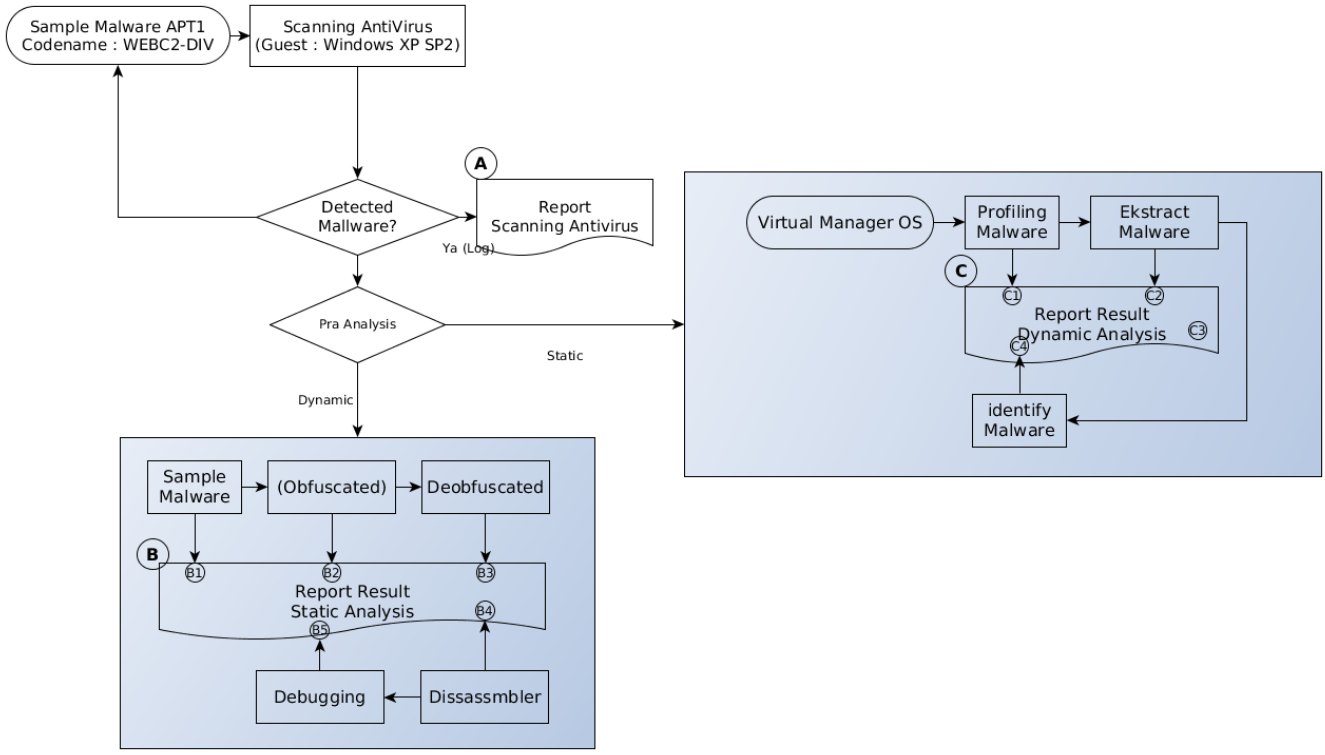
4. Analisis

Diajukan skema statis, penelitian forensic malware host dan guest Windows XP SP3. Host fisik memiliki IP 192.168.56.1 dan guest ruang linkup malware akan dijalankan memiliki IP 192.168.56.101. Seperti tertera pada gambar berikut :



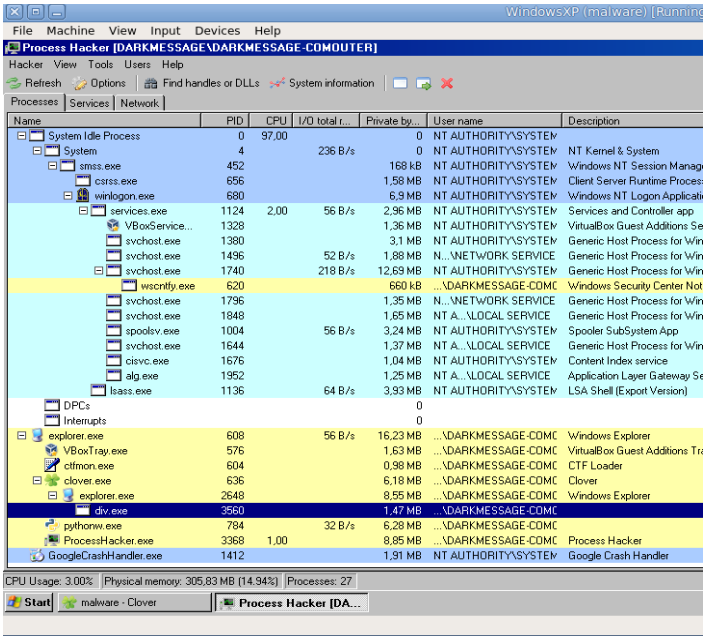
Gambar 1 process model forensic WEBC2-DIV

Analisis malware, terdapat dua pokok utama teknik yang sering digunakan diantaranya analisis statis dan dinamis. Analisis statis merupakan metode malware tanpa menjalankan, analisis ini menggunakan metode yang lebih aman dari dinamis. Ditunjukkan pada Gambar 2



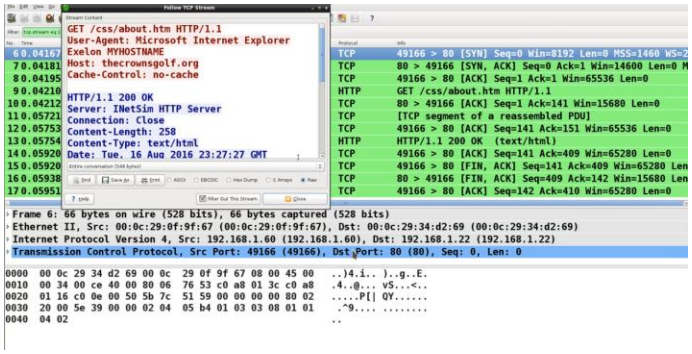
Gambar 2 Lingkup kerja analisis malware WEBC2-DIV

Malware WEBC2-DIV dijalankan pada guest, pada baris warna biru tampak seperti gambar berikut :



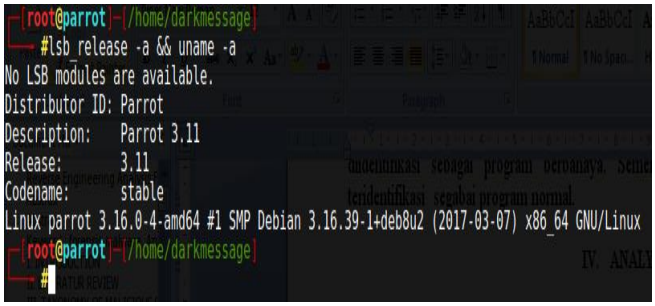
Gambar 3 Proses Hacker menentukan WEBC2-DIV

Setelah div.exe berjalan pada guest, wiresark pada host mencoba mencari melaui jaringan, string cleartext yang didapatkan dan terdapat malware mencoba terhubung pada korban melalui dns malicious thecrowngolf.org Gambar 4



Gambar 4 host malware WEBC2-DIV

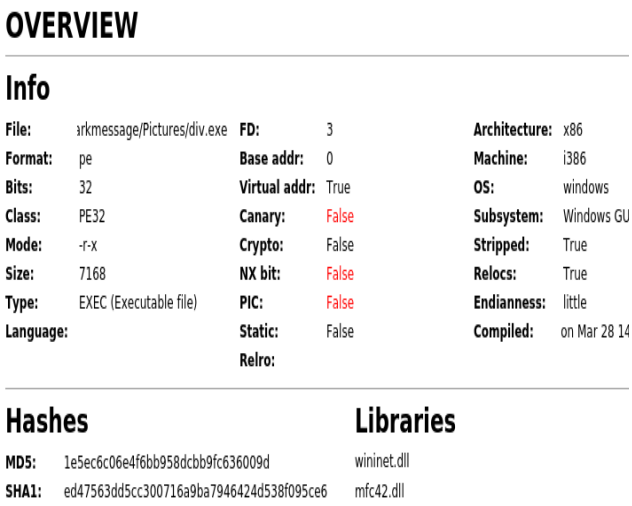
Sebelum melakukan teknik reverse engineering, komputer yang digunakan untuk melakukan disambler pada sistem operasi ParrotOS dan kernel 3.16.0-4 Gambar 5



Gambar 5 Host dissambler

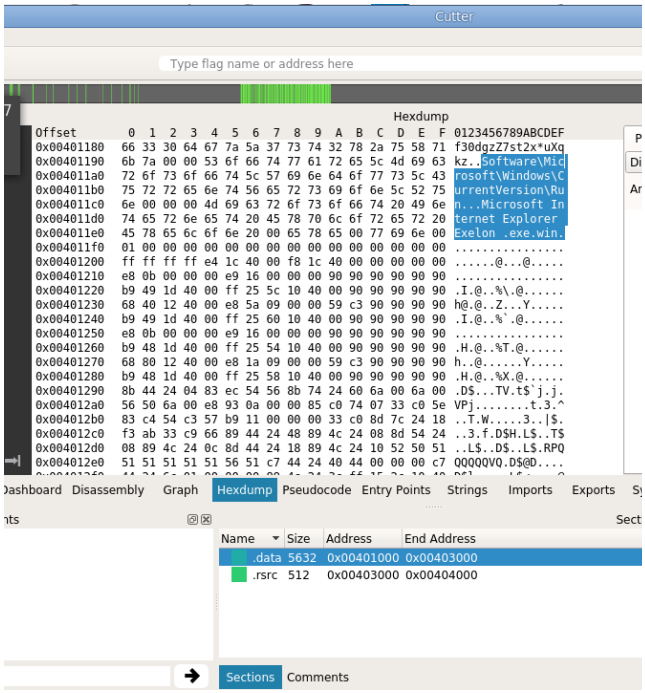
File malware div.exe, ikhtisar teknik reverse engineering diawali dengan mencari informasi mengenai Malware WEBC2-DIV tersebut, pencarian informasi menggunakan Software Cutter yang dijalan kan didapatkan berupa

infromasi, hash dan library apa saja yang didapatkan. Seperti Gambar 6



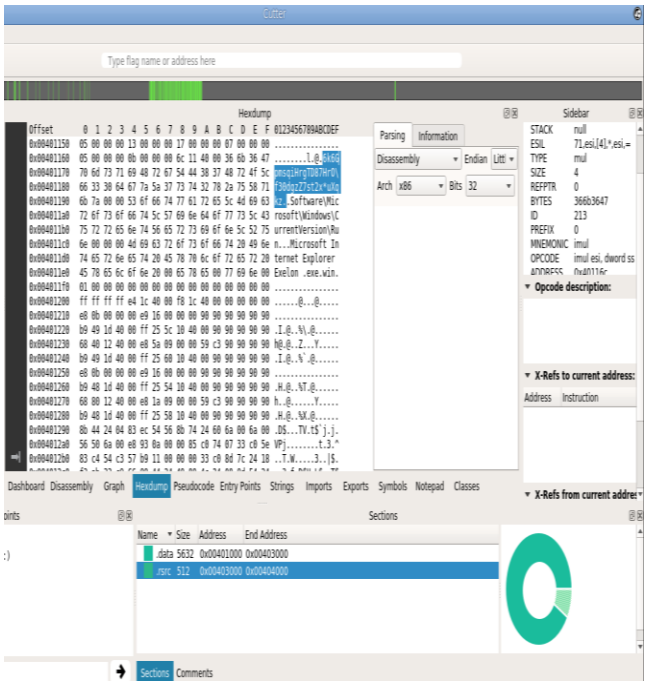
Gambar 6 Overview Malware WEBC2-DIV

Saatnya melakukan dissamble pada badan malware sehingga didapatkan bahwa tingkah laku malware berinang pada host dan melakukan penanaman nilai pada regedit windows beralamat HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Run. Dapat dilihat pada blok warna seperti Gambar 7.

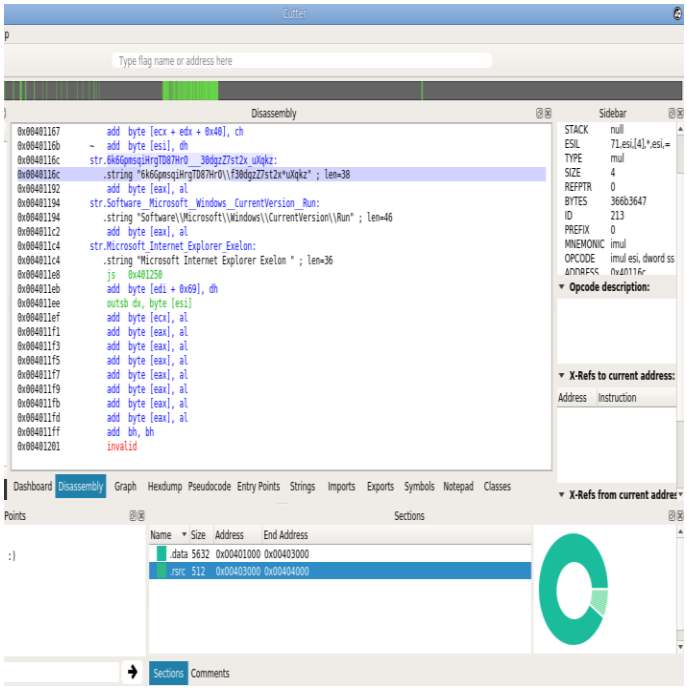


Gambar 7 Pengalamatan malware pada regedit windows

Tidak hanya sampai disini pada malware WEBC2-DIV didapatkan sebuah enkripsi yang menyimpan informasi penting untuk melumpuhkan sistem keamanan komputer yang di infeksi. Seperti warna blok Enkripsi seperti pada Gambar 8 dan Gambar 9.

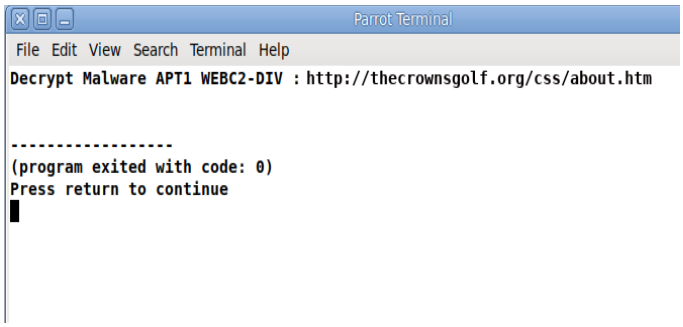


Gambar 8 HexDump nilai encrypt malware WEBC2-DIV



Gambar 9 Nilai string WEBC2-DIV encrypt pada disassembly

Decode enkripsi untuk mendapatkan informasi tingkah laku malware. Dengan hal in bisa mengetahui lebih dalam apa saja yang diinginkan pencipta malware terhadap infeksi sistem keamanan komputer client. Hasil decode didapatkan seperti Gambar 10.



Gambar 10 decode string encrypt

5. Kesimpulan

Malware WEBC2-DIV merupakan malicious software terbaik saat melakukan spionasi kegiatan yang dilakukan diantaranya :

1. Phising email.
2. Phising login credential.
3. Menyusupkan backdoor
4. Melakukan remote.

Empat hal tersebut menjadi dasar, Malware ini menjadi efektif saat melakukan spionasi dan pamor sejak tahun 2010. Tidak menutup kemungkinan malware WEBC2-DIV melakukan update pada fungsi dan kegiatan yang dilakukan oleh sipembuat. Serta melakukan enkripsi lebih dalam pada tubuh malware.

Hal kedepan yang menjadi suatu tantangan automatisasi, mengenal malware melalui hash yang ada serta melakukan clustering terhadap jenis malware tersebut. Untuk menjadi sebuah trobosan terbaru dalam melakukan pengenalan malware melalui cara pindai.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Direktorat Riset dan Pengabdian Masyarakat, Direktorat Jenderal Penguatan Riset dan Pengembangan, Kementerian Riset Teknologi dan Perguruan Tinggi yang telah memberi dukungan terhadap penelitian ini.

Daftar Pustaka

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.

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

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

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

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

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.

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

H, J. K. (2008). Code graph for malware detection, in:Information Networking. *ICOIN (International Conference)* , 1-5.

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

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.

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).

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

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

Raditya, W. F. (2013). Rancang Bangung Aaplikasi Uuntuk Menyerang Balik dari Pengguna Netcut Dijaringan Lokal Menggunakan DDos. *Skripsi, Fakultas Ilmu Komputer*.

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.

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

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

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

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