ANALISIS MALWARE PADA SISTEM OPERASI WINDOWS MENGGUNAKAN TEKNIK FORENSIK

Yuriansyah Ilhamdi [1], Yesi Novaria Kunang[2]
Fakultas Ilmu Komputer, Universitas Bina Darma
Email: yuriansyailhamdii@gmail.com [1], yesi_novariakunang@binadarma.ac.id [2]

ABSTRAK

Malware merupakan perangkat lunak atau *software* yang diciptakan untuk menyusup atau merusak sistem komputer. *malware* adalah sejenis program komputer yang dimaksudkan untuk mencari kelemahan *software* sehingga pada perangkat akan terkena *virus*, malware dapat berisi kode berbahaya seperti *Virus*, *Worm*, *Trojan Horse*. Penyebaran *malware* saat ini begitu mudah baik melalui usb *flashdisk*, iklan-iklan tertentu pada *website*, dan media lainnya. *Windows* merupakan salah satu sistem operasi yang paling banyak di gunakan, dengan jumlah pengguna dan penyedia aplikasi di internet yang banyak, memungkinkanpenyebaran *malware* pada *windows* mudah untuk dilakukan. Metodologi yang di gunakan dalam penelitian ini adalah *malware dynamic analysis*. Penelitian ini nantinya akan menghasilkan informasi mengenai aktivitas dan pola serangan *malware*, yang di harapkan dapat membantu pengguna sistem operasi *windows* untuk mengantisipasi ancaman dan serangan *malware*

Kata kunci: *Malware, Dynamic Analysis, Forensik, Windows, Cyber Crime*

ABSTRACT

Malware is software or software created to infiltrate or damage computer systems. Malware is a type of computer program that is intended to look for software weaknesses so that the device will be exposed to viruses, malware can contain malicious code such as viruses, worms, Trojan horses. Currently, the spread of malware is easy, both via USBflash drives, certain advertisements on websites, and other media.Windows is one of the most widely used operating systems, with a large number of users and application providers on the internet, making it easy to spread malware on windows. The methodology used in this research is dynamic malware analysis. This research will produce information about the activity and pattern of malware attacks, which are expected to help users of the Windows operating system to anticipate threats and malware attacks.

Keyword: *Malware, Dynamic Analysis, Forensik, Windows, Cyber Crime*

1. PENDAHULUAN

Dalam perkembangan teknologi, komputer dan internet menjadi salah satu kebutuhan bagi manusia, dengan tingginya penggunaan komputer dan internet tentu saja menjadi tantangan dan ancaman dari kejahatan, kejahatan tak hanya terjadi di dunia nyata namun juga merambah ke dunia

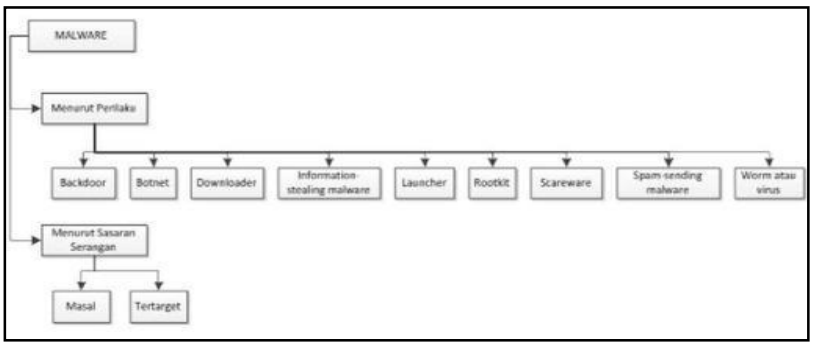
maya yang sering di sebut dengan kejahatan siber. Cara pelaku dalam melakukan tindak kejahatan siber ini beragam, salah satu cara pelaku untuk melakukan tindak kejahatan tersebut diantaranya melibatkan *malware*.

Malware merupakan perangkat lunak atau software yang diciptakan untuk menyusup atau merusak sistem komputer. *Malicious Software* atau di sebut dengan malware merupakan suatu program yang bertujuan untuk merusak, mengambil atau mengubah data-data yang dimiliki orang lain dengan tujuan tertentu, agar informasi-informasi yang didapat di manfaatkan untuk kejahatan. *Malware* berbentuk program yang dapat mengeksploitasi file-file penting dalam komputer. Ada bermacam-macam jenis *malware* di antaranya yaitu *worm, Trojan, ransomeware, backdoor,* dan lainnya. *Malware* biasanya di sebarkan melalui aplikasi, para pelaku biasanya melakukan penyebaran *malware* melalui aplikasi illegal yang banyak beredar di *internet*, dengan cara mensisipkan *malware* pada perangkat lunak illegal tersebut, korban di kelabui dengan menginstal perangkat lunak yang sudah di sisipkan *malware*.

Salah satu sitem operasi yang sering menjadi target dari penyebaran *malware* adalah sistem operasi *windows*. *Malware* itu sulit untuk di deteksi teknik untuk mengamati malware di dalam sistem operasi disebut dengan teknik *forensic malware*, dengan metode *malware dynamic analisis.* Kelebihan dari analisa dinamis ini adalah ketika program atau software yang di identifikasi memiliki kode binary yang sifatnya rumit dan tidak dapat dilakukan analisa secara statis sehingga dengan menganalisa tingkah laku saat proses runtime ketika program ataupun software dieksekusi akan terlihat karakteristik maupun tingkah laku program tersebut maka dapat ditentukan apakah software atau program tersebut dikategorikan sebagai malware atau bukan. Yang mana pada proses analisisnya membutuhkan pengeksekusian terhadap contoh *malware* untuk kemudian dipelajari perilaku yang ditimbulkan oleh *malware* tersebut sehingga dapat diperoleh informasi tentang bagaimana sebuah *malware* tersebut bisa berkembang atau memanipulasi dirinya sendiri, dan pada komponen sistem apa saja *malware* tersebut berkomunikasi. Metode ini dilakukan dengan carayaitu menjalankan *malware* pada *OS virtual*, sehingga apabila *malware* yang dijalankan tersebut ternyata merusak sistem, maka sistem utama tidak mengalami kerusakan akibat *malware* tersebut.

Malware mepakan singkatan dari *malicious software*, yaitu sebuah sebutan bagi *software* yang didesain sedemikian rupa agar dapat menyusup ke dalam sebuah sistem komputer tanpa diketahui pemilik sistem, dimana di dalam *software* tersebut terdapat perintah perintah khusus yang dibuat dengan tujuan khusus, seperti menyebarkan *virus, trojan, worm,* atau memasang *backdoor.* Secara umum dapat dikatakan bahwa, *malware* merupakan aplikasi yang dapat atau akan membuat celah pada keamanan sebuah system Komputer (Perdana, 2011). *Malware (Malicious Software)* merupakan program yang dirancang untuk disusupkan ke dalam sebuah sistem dengan tujuan untuk melakukan beraneka ragam aktivitas yang bersifat merugikan pemiliknya. Merugikan dalam arti kata dampak negatif yang ditimbulkan dapat berkisar mulai dari sekedar memperlambat kinerja sistem hingga merusak bahkan menghancurkan data penting yang tersimpan dalam sistem (Manoppo et al., 2020). *Malicious software* atau yang biasa dikenal dengan *malware* merupakan sebuah perangkat lunak yang terpasang pada suatu sistem komputer tanpa sepengetahuan oleh *user* atau pemilik sistem tersebut (Aslan, 2017).

Sesuai dengan namanya, *malware* dapat melakukan *malicious action* atau tindakan jahat seperti mencuri informasi rahasia, perusakan pada suatu sistem, mendapatkan hak akses suatu komputer dan menjalankan program yang ada pada komputer tersebut. Setiap perangkat lunak yang melakukan sesuatu yang dapat menyebabkan kerugian pada *user*, komputer ataupun jaringan dapat dianggap sebagai *malware* (Sikorski, M., 2012).



Gambar 1. Taksonomi *Malware*

Malware dapat dikategorikan menjadi beberapa jenis dan *malware* mempunyai banya variasi juga, antara lain adalah (Nate, 2012).

a. Adware. Adware mempunya kepanjangan *advertising-supported software,* adalah jenis *malware*yang secara otomatis mengirimkan iklan yang menarik perhatian kepada *user*, seperti contohnya *pop-up* iklan pada *website* tertentu, kadang *adware* juga menawarkan aplikasi yang gratis namun saat di unduh berisikan *malware* lain atau *adware* itu sendiri.

b. Botnet. Bot atau *botnet* adalah sebuah *software* yang diprogram dan dirancang untung melakukan sebuah aktivitas atau operasi secara otomatis, seperti misalnya pada serangan jaringan *DDoS (Distributed Denial of Service) botnet* digunakan untuk melakukan *ping* kepada *victim* yang sudah di tentukan, *botnet* dapat beroperasi secara otomatis dan dapat juga di kontrol oleh pihakketiga.

c. Bug. Bug merupakan sebuah kejanggalan atau kesalahan pada suatu program yang biasanya tercipta karna kesalahan pembuatnya sendiri dalam memasukan barisan kode saat pembuatan sebuah program, namun bug dapat menjadi alasan kenapa sebuah program berjalan tidak sesuai yang diinginkan bahkan saat tidak teridentifkasi pada jangka waktu yang lama juga dapat menyebabkan kelemahan atau celah yang dapat di eksploitasi.

d. Ransomware. Ransomware adalah jenis malware yang saat diaktifkan akan mengunci sistem operasi dan data user sebagai tawanan dan data tidak akan diberikan kembali sampai tebusan yang sudah ditentukan sudah dibayar. *Malware* ini membatasi hak akses *user* dan mengenkripsi *file* yang ada pada *hard drive*, dan menampilkan pesan yang bertujuan untuk memaksa *user* membayar tebusan.

e. Rootkit. Rootkit adalah sebuah malware yang memungkinkan *hacker* melakukan *remote access control* tanpa terdeteksi user aslinya. Ketika *rootkit* diaktifkan akan memungkinkan *hacker* mengeksekusi *file*, mengakses dan mencuri informasi secara diam-diam, karna *rootkit* sulit untuk terdeteksi maka *rootkit* sangatlah berbahaya.

f. Spyware. Spyware adalah jenis malware yang berfungsi untuk memata-matai aktivitas user tanpa useritu sendiri mengetahui, malware ini bertujuan untuk mengetahui aktivitas *user*, dan memanen informasi terkait finansial seperti misalnya transaksi bank yang sensitif untuk diketahui.

g. Trojan Horse. Trojan horse atau biasa disebut *trojan* adalah sebuah malware yang mempunyai metode menyembunyikan malware nya di dalam file biasa guna menipu user, ketika *file* telah *ter- install* maka *malware* yang berada dalam *file* tersebut akan diaktifkan, *malware* ini dapat memberi akses *remote* pada *hacker* dan memungkinkan pencurian

informasi bahkan sampai pencurian uang elektronik

h. *Virus.* Virus adalah malware yang dapat menduplikat dirinya sendiri dan menyebar ke komputer lain ketika telah diaktifkan, virus dapat menyebar ke komputer lain dengan menempelkan dirinya ke beberapa program tertentu yang nantinya diaktifkan di komputer lain. Virus dapat digunakan untuk mencuri informasi, mencuri uang elektronik, membuat *botnet*, merusak *host* dan juga jaringan.

i. *Worm. Worm* adalah satu diantara malware yang paling umum, *worm* menyebar melalui jaringan komputer dengan melakukan eksploitasi terhadap celah yang ada pada sistem operasi. *Worm* pada umumnya menyebabkan rusak nya *host* dengan mengkonsumsi banyak bandwidth dan mengisi *web server* sampai *overload*.

Ada beberapa cara yang dapat di gunakan untuk menganalisa malware yang ada di komputer salah satunya dengan menggunakan teknik forensik. *digital forensic* merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepetingan pembuktian hukum *(pro justice)*, yang dalam hal ini untuk membuktikan kejahatan berteknologi tinggi atau *computer crime* secara ilmiah *(scientific)* hingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut. (Alzahar, 2012). menurut (Luz Yolanda Toro Suarez, 2015) Forensik digital merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital.

Dynamic analysis yang pada proses analisisnya membutuhkan pengeksekusian terhadap contoh *malware* untuk kemudian dipelajari perilaku yang ditimbulkan oleh *malware* tersebut sehingga dapat diperoleh informasi tentang bagaimana sebuah malware tersebut bisa berkembang atau memanipulasi dirinya sendiri, dan pada komponen sistem apa saja malware tersebut berkomunikasi (Bayer, Kirda, & Kruegel, 2010; Bayer, Moser, Kruegel, & Kirda, 2006; *Education, Science*, Sujyothi, & Acharya, 2017; Egele, Scholte, Kirda, & Kruegel, 2012). Sedangkan Menurut (Adenansi & Novarina, 2017) Analisis dinamik merupakan metode analisa yang mengamati kerja suatu sistem yang dapat terlihat dari perilaku suatu sistem sebelum *malware* dijalankan dengan perilaku setelah *malware* tersebut dijalankan atau dieksekusi dalam sistem tersebut.

Ada tahapan yang akan dilakukan dalam menganalisa *malware* menggunakan metode *dynamic analysis* yaitu.

1) *Malware Defined*, yaitu mengklasifikasi tipe dan jenis sample *malware*.
2) MEAR (*Malware Analysis Environtment and Requirement),* merupakan pembahasan yang mengarah pada kebutuhan seorang peneliti *malware* dalam melakukan penelitian terhadap *malware*. Komponen yang ada di dalam MEAR antara lain: *malware source, virtual machine.*
3) *Malware Identification*, merupakan proses identifikasi terhadap *malware* dengan melakukan *monitoring* dari prilaku *malware* untuk mengetahui bagaimana *malware*berinteraksi dengan sistem.

Menentukan ruang lingkup penelitian yang akan dilakukan pada lingkungan aman dimana menggunakan lingkungan *virtual* untuk pengujian sample virus. Lingkungan mesin *virtual*atau yang lebih dikenal dengan *virtual* mechine (VM). *Virtual Machine* Ide dasar dari mesin *virtual* adalah mengekstraksi perangkat keras seperti CPU, memori, disk drive ke beberapa *environment* sehingga menciptakan ilusi bahwa masing-masing environment tersebut menjalankan komputernya sendiri. Meskipun secara fisik tidak memiliki *hardware* tersebut. VM muncul karena adanya keinginan untuk menjalankan beberapa sistem operasi pada satuperangkat keras tertentu. Sistem VM memungkinkan pembagian sumber daya perangkat keras yang ada ke tiap-tiap VM yang berbeda. Dengan teknologi virtualisasi, maka sebuah komputer tunggal bisa menjalankan beberapa komputer virtual secara simultan dan bersama-sama. Lapisan perangkat lunak yang menyediakan virtualisasi

disebut VMM atau *Virtual Machine Monitor*. Diatas VMM dapat diinstall sebuah *guest software* (sistem operasi dan aplikasi). VMM akan menyediakan abstraksi hardware untuk *guest software* ini menggunakan *emulated hardware*. Selanjutnya *Guest software* akan berinteraksi dengan *hardware virtual* dengan cara yang sama seperti berinteraksi dengan hardware yang sebenarnya. Contohnya pada instruksi in/out, DMA, dan lain-lain. Semua *guest software* (termasuk sistem operasi) bekerja pada mode *user*, sedangkan VMM beroperasi pada *level kernel*. VMM akan mengisolasi semua sumber daya dari masing-masing mesin *virtual* dalam berhubungan secara langsung. (Najoan, 2012)

Process Monitor digunakan untuk memonitor pembuatan atau penghentian proses atau memberikan informasi lebih banyak kepada analis tentang proses tertentu. Alat inimenggabungkan fitur dari dua *utilitas Sysinternals* (*Regmon* dan *Filemon*) dan menambahkan kemampuan pemfilteran. Fitur-fitur ini menjadikan *Process Monitor* sebagai alat penting yang harus disertakan oleh setiap analis dalam menganalisa *malware*.

2. METODOLOGI PENELITIAN

2.1 *Persiapan*

Pada penelitian ini digunakan metode penelitian *dynamic analysis* yang pada proses analisisnya membutuhkan pengeksekusian terhadap contoh *malware*. Berikut adalah tahapan dalam metode *dynamic analysis*: Pada tahap ini menyusun rencana kegiatan agar penelitian dapat dilakukan dengan baik dan lancar, pada penelitian ini akan dilakukan analisis malware pada system operasi *windows*. menjalankan *malware* pada sebuah sistem operasi *windows virtual* di dalam *virtual box*, lalu mengamati aktivitas yang dilakukan oleh malware dengan menggunakan *software* yang sudah disiapkan.

2.2 *Perencanaan*

Pada tahapan perencanaan dalam penelitian ini ada beberapa kebutuhan yang harus dipersiapkan sebelum melakukan analisis *malwar*e pada sistem operasi *windows* 10 yaitu alat berupa perangkat keras dan perangkat lunak.

2.3 *Alat Penelitian*

Tabel 1. Perangkat Keras dan Perangkat Lunak

Hardware	Software
1 Laptop	Windows 10 Regshot Process Monitor

2.4 *Malware Defined*

Tahap pertama dalam analisa *malware* adalah mengklasifikasikan *type* dan jenis sample *malware*. Pada penelitian ini sample *malware* di download dapat di VirusShare.com. Berikut adalah sample *malware* yang di gunakan dalam penelitian ini.

Tabel 2. Nama dan Jenis Sampel Malware

Nama	Jenis
TrojWare.Win32.Kryptik.VA	Trojan Horse
RA	Trojan
Trojan.GenericKD.40437260	HorseTrojan
Trojan\Win32.VBKrypt	Horse
Backdoor.Win32.Zegost	Backdoor
Trojan.Delf.Agent.HZ	Trojan
Backdoor.Agent.ABWI	Horse
	Backdoor

2.5 MEAR (*Malware Analysis Environtment and Requirement)*

Komponen yang ada didalam MAER yaitu *sample malware* dan *virtual lab*. Pada penelitian ini*virtual lab* yang di gunakan adalah *virtual box*, dan sample *malware* yang akan di analisis yaitu *trojan* dan *backdoor.*

3. HASIL DAN PEMBAHASAN

Dari keenam *malware* yang di analisis, *malware TrojWare.Win32Kryptik.VARA* adalah malware yang paling berbahaya karena yang paling merusak file sistem, memiliki *file generate* paling banyak, penggunaan cpu yang besar yaitu sebesar 100%, dan menggunakan *resource memori* yang paling besar diatara ke 6 *malware* yang telah di analisis yaitu sebesar 323,47 MB.

Tabel 3. Hasil Penelitian

(A = Addedvalue, B = CreateFile, C = ReadFile, D = Duplikasi, E = WriteFile, F = CloseFile, G = LockFile)

Malware	Reg shot	Process Monitor						CPU Usage	Memoy Usage
	A	B	C	D	E	F	G		
TrojWare.Win32Kryptik.VARA	√	√	√	√	√	√	√	100%	323,47 MB
Trojan.GenericKD.40437260	√	√	√			√		97.84%	65,85 MB
Trojan\Win32.VBKrypt	√	√	√			√		56.48%	1,18 MB
Backdoor.Win32.Zegost	√	√				√		53.13%	4,19 MB
Trojan.Delf.Agent.HZ	√	√				√		97.80%	128,38 MB
Backdoor.Agent.ABWI	√	√	√			√		79.13%	1,01 MB

1) *Malware TrojWare.Win32Kryptik.VARA*

Melakukan create file pada sistem yaitu *net.exe, sysmain.sdb,help, KavUpda.exe,HelpCat.exe, dan at.exe. Malware TrojWare.Win32Kryptik.VARA* juga dapat menduplikasi diri yaitu *KavUpda.exe* dan *HelpCat.exe.* Kemudian *malware TrojWare.Win32Kryptik.VARA* melakukan read file pada sistem yaitu *oleaut32.dll, net.exe, KavUpda.net, at.exe, sc.exe, sysmain.sdb, regedit.exe, dan reg.exe.* Lalu *Malware TrojWare.Win32Kryptik.VARA* juga melakukan write file pada sistem yaitu *Sysinf.bat, regedit32.sys, msedge.exe, msedge_proxy.exe, pwahelper.exe, dan cookie_exporter.exe.* Selain write file *malware TrojWare.Win32Kryptik.VARA* juga melakukan lock file yaitu *DF4C9311DB601ECF92.TMP.* Penggunaan CPU oleh *malware TrojWare.Win32Kryptik.VARA* pada sistem sebesar 100% dan penggunaan memori sebesar 323,47 MB.

2) *Malware Trojan.GenericKD.40437260*

Melakukan create file pada sistem yaitu *combase.dll, oleout32.dll, msvbvm60.dll, imm32.dll,edgegdi.dll, SortDefault.nls, shell32.dll, crypt32.dll, netapi32.dll, netutils.dll, ws2_32.dll, NapiNSP.DLL, pnrpnsp.dll, dan wshbth.dll.* Lalu read file pada sistem yaitu *apphelp.dll, msvbvm60.dll, ole32.dll, oleaut32.dll, dan StaticCache.dat.* Malware *Trojan.GenericKD.40437260* juga melakukan close file yaitu *gdi32full.dll, gdi32.dll, user32.dll,*

msvcrt.dll, rpcrt4.dll, sechost.dll, advapi32.dll, combase.dll, ole32.dll, oleaut.dll, imm32.dll, SortDefault.nls, shell32.dll, netapi32.dll, netutils32.dll, dan, NapiNSP.dll. Malware Trojan.GenericKD.40437260 tidak melakukan write file dan lock file serta penggunaan CPU pada sistem sebesar 97,84% lalu penggunaan memori pada sistem sebesar 65,85 MB.

3) *Malware Trojan\Win32.VBKrypt*

Malware melakukan create file *apphelp.dll, ntdl.dll, KernelBase.dll, kernel32.dll, sysmain.sdb, win32u.dll, ucrtbase.dll, user32.dll, mm32.dll, sechost.dll, combase.dll, dan SortDefault.nis.* Kemudian melakukan read file pada sistem yaitu *apphelp.dll dan msvbvm60.dll, malware* juga melakukan close file yaitu *apphelp.dll, ntdl.dll, kerne32.dll, KernelBase.dll, sysmain.sdb, win32u.dll, user32.dll, imm32.dll, msvbvm60.dll, advapi32dll, combase.dll, ole32.dll, dan SortDefault.nis. Malware Trojan\Win32.VBKrypt* Tidak melakukan duplikasi, write file, dan lock file. Penggunaan CPU pada sistem sebesar 56,48% serta penggunaan memori sebesar 1,18MB.

4) *Malware Backdoor.Win32.Zegost*

Melakukan create file yaitu *apphelp.dll, ntdll.dll, kernel32.dll, kernelbase.dll, sysmain.sdb, AcGenral.dll, uxtheme.dll, winmm.dll, samcli.dll, msacm32.dll, verdion.dll, userenv.dll, winspool.dll, mpr.dll, winmmbase.dll ,jertutil.dll* dan *AcLayer.dll. Malware Backdoor.Win32.Zegost* juga melakukan close file pada sistem yaitu *apphelp.dll, ntdl.dll, kernel32.dll, kernelbase.dll, sysmain.sdb, AcGenrel.dll, uxtheme.dll, winmm.dll, samcli.dll, msacm32.dll, version.dll, userenv.dll, dwmapi.dll, urlmon.dll, dan winspool.drv. Malware Backdoor.Win32.Zegost* tidak melakukan read file, duplikasi, dan lock file. Penggunaan CPU pada sistem sebesar 53.13% serta pemggunaan memori pada sistem sebesar 4,19 MB.

5) *Malware Trojan.Delf.Agent.HZ*

Melakukan create file yaitu *sysmain.sdb, version.dll, winspool.drv,*

win32u.dll,ucrtbase.dll,msvcp_win.dll, gdi32full.dll, gdi32.dll, user32.dll, rpcrt4.dll, dan sechost.dll.Malware Trojan.Delf.Agent.HZ juga melakukan close file yaitu *apphelp.dll, ntdl.dll,*
kernel32.dll,bf34c8ed9467299cb2c7d711e63ab460e4039d5355ef76eb1dgc73b51b0ef637.exe, kernelbase.dll, sysmain.sdb, version.dll, winspool.drv, win32.dll,ucrtbase.dll, msvcp_win.dll,gdi32full.dll, user32.dll, sechost.dll, dan advap32.dll. Malware Trojan.Delf.Agent.HZ tidakmelakukan read file, duplikasi, write file, dan close file.

Penggunaan CPU pada sistem sebesar97,80% serta penggunaan memori sebesar 128,38 MB.

6) *Malware Backdoor.Agent.ABWI*

Melakukan create file yaitu *System32, edgegdi.dll, oleaut32.dll, winhttp.dll, IPHLPAPI.DLL, rpcss.dll, kernel.appcore.dll, ncrypt.dll, ntasn1.dll, windows.storage.dll, wldp.dll, SortDefault.nis, dan taskschd.dll. malware Backdoor.Agent.ABWI* juga melakukan read file yaitu *clien_id* dan *malware Backdoor.Agent.ABWI* juga melakukan close file yaitu *oleaut32.dll, winhttp.dll, IPHLPAPI.DLL, rpcss.dll, kernel.appcore.dll, ncrypt.dll, wldp.dll, ncrypt1.dll, windows.storage.dll, dan taskschd.dll. malware Backdoor.Agent.ABWI* tidak melakukan duplikasi, write file, dan lock file. Penggunaan CPU pada sistem sebesar7 79,13% dan penggunaan memori sebesar 1,01 MB.

4. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan oleh penulis di penelitian ini, penulis menarik kesimpulan yaitu, kita dapat mengetahui pola aktifitas dan bagaimana *malware* menyerang dan mengekploitasi file pada komputer serta merusak file sistem pada sistem operasi *windows*. Diharapkan dari hasil penelitian ini dapat bermanfaat dalam mendeteksi serta mengantisipasi serangan *malware* bagi pengguna sistem operasi *windows.*

Beberapa saran yang diusulkan oleh penyusun untuk penelitian lebih lanjut sebagai berikut :

1) *Malware* merupakan topik yang masih sangat terbuka luas untuk penelitian, padapenelitian ini penulis menggunakan metode *dinamic analysis*, maka penulis menyarankan untuk penelitian kedepannya menggunakan teknik analisis *malware* dengan metode *static analysis* yang tidak di gunakan pada penelitian ini.
2) *Tools* yang di gunakan pada penelitian ini tidak terlalu akurat dalam mendeteksi,sehingga perlunya perbaikan pada penelitian selanjutnya
3) Untuk penelitian kedepan dapat menggunakan *tools* analisa *malware* lainnya agar dapat membantu mengetahui karakteristik dari sebuah *malware* secara spesifik.

DAFTAR PUSTAKA

Adenansi, R., & Novarina, L. A. (2017). Malware dynamic. *Jurnal of Education and Information Communication Technology*, *1*(1), 37–43.

Alzahar, M. N. (2012). *Digital Forensik: Panduan Praktis Investigasi Komputer*. Salemba. Aslan, O. (2017). Performance Comparison of Static MalwareAnalysis ToolsVersusAntivirus Scanners To Detect Malware Performance Comparison of Static Malware Analysis Tools Versus Antivirus Scanners To Detect Malware. *International Multidisciplinary Studies Congress*.

Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2012). A survey on automated dynamic malware-analysis techniques and tools. In *ACM Computing Surveys*. https://doi.org/10.1145/2089125.2089126

Luz Yolanda Toro Suarez. (2015). *SEKILAS MENGENAI FORENSIK DIGITAL*. 1–27.

Manoppo, V. A., Lumenta, A. S. M., Karouw, S. D. S., Elektro, J. T., Sam, U., Manado, R.,& Bahu, J. K. (2020). *Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi*. *9*(3), 181–188.

Najoan, X. (2012). Analisis Aspek Keamanan Dalam Menghadapi Rootkit Berbasis Mesin Virtual (VMBR). *Jurnal Teknik Informatika*. https://doi.org/10.35793/jti.1.1.2012.545

Nate, L. (2012). *Common Malware Types: Cybersecurity 101*. 15 Oktober 2012. Netmarketshare.com. (2016).

Perdana, M. R. (2011). *Harmless Hacking: Malware Analisis dan VulnerabilityDevlopment*. Penerbit Graha Ilmu.

Savira, F., & Suharsono, Y. (2013). *Journal of Chemical Information and Modeling*,*01*(01).

Sikorski, M., & H. (2012). *Practical Malware Analysis*. William Pollock.

Wardhana, S. R. (2014). *Analisa hybrid untuk sistem deteksi malware otomatis dengan support vector model classifier*. 1–10.