SKRIPSI

APLIKASI PENDETEKSI MALWARE DENGAN TEKNIK ANALISIS DINAMIS

ADAM HAFIDZ FITRASANI

NPM: 2013730067

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN SAINS
UNIVERSITAS KATOLIK PARAHYANGAN

2017

UNDERGRADUATE THESIS

MALWARE DETECTOR APPLICATION WITH DYNAMIC ANALYSIS TECHNIQUE

ADAM HAFIDZ FITRASANI

NPM: 2013730067

DEPARTMENT OF INFORMATICS
FACULTY OF INFORMATION TECHNOLOGY AND SCIENCES
PARAHYANGAN CATHOLIC UNIVERSITY
2017

LEMBAR PENGESAHAN

APLIKASI PENDETEKSI MALWARE DENGAN TEKNIK ANALISIS DINAMIS

ADAM HAFIDZ FITRASANI

NPM: 2013730067

Bandung, 22 Mei 2017

Menyetujui,

Pembimbing

Dr. Veronica Sri Moertini 2-8-2017

Ketua Tim Penguji	Anggota Tim Penguji
Mariskha Tri Adithia, P.D.Eng	Aditya Bagoes Saputra, M.T.

Mengetahui,

Ketua Program Studi

Mariskha Tri Adithia, P.D.Eng

PERNYATAAN

Dengan ini saya yang bertandatangan di bawah ini menyatakan bahwa skripsi dengan judul:

APLIKASI PENDETEKSI MALWARE DENGAN TEKNIK ANALISIS DINAMIS

adalah benar-benar karya saya sendiri, dan saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan.

Atas pernyataan ini, saya siap menanggung segala risiko dan sanksi yang dijatuhkan kepada saya, apabila di kemudian hari ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya, atau jika ada tuntutan formal atau non-formal dari pihak lain berkaitan dengan keaslian karya saya ini.

Dinyatakan di Bandung,
Tanggal 22 Mei 2017

Adam Hafidz Fitrasani
NPM: 2013730067

ABSTRAK

Pada masa kini, pemakaian komputer, notebook dan sebagainya sudah sangat banyak. Ada banyak sistem operasi yang digunakan oleh perangkat-perangkat tersebut, contohnya adalah Ubuntu, Debian, dan Windows. Saat ini yang paling umum digunakan di dunia ini adalah sistem operasi Windows. Pada sistem operasi Windows, banyak aplikasi yang dapat digunakan untuk membantu aktifitas tertentu. Contohnya adalah aplikasi pengolah kata, peramban internet, dan pengolah data. Terkadang, ada aplikasi berbahaya yang melakukan aktifitas-aktifitas yang membahayakan sistem yang berjalan. Aktifitas yang dilakukan oleh aplikasi tersebut bersifat tersembunyi sehingga jika aplikasi tersebut melakukan suatu perubahan, perubahan tersebut tidak terdeteksi oleh pengguna. Biasanya, perangkat lunak yang mendeteksi ini tidak menyimpan data perubahan apa saja yang dilakukan oleh aktifitas tersembunyi tersebut. Aktifitas tersembunyi biasanya adalah meng-edit sebuah *file*, meng-copy *file*, menghapus *file*, mengirim *file* melalui jaringan, mengakses jaringan tertentu atau situs tertentu. Walaupun aktifitas-aktifitas tersebut merupakan hal yang normal, aktifitas tersebut bisa menjadi berbahaya jika aktifitas-aktifitas yang disebutkan di atas dilakukan tanpa sepengetahuan pengguna dan *file* yang digunakan di dalam aktifitas tersebut merupakan *file* sistem atau *file* penting milik pengguna. Ada kemungkinan juga aplikasi yang berbahaya itu akan mengakses situs-situs atau jaringan yang berbahaya, misalnya situs-situs yang ketika diakses akan mengunduh *malware*.

Tujuan dari penelitian yang dibuat adalah untuk membuat aplikasi yang dapat mencatat aktifitas *malware* terhadap sistem, dan mengirimkan pesan ke server terkait dengan aktifitas *malware* yang dilakukan di komputer tersebut. Dengan demikian komputer yang dipantau dapat diketahui bagian mana saja yang diubah oleh *malware*.

Analisis dinamis adalah analisis yang menggunakan tingkah laku dari suatu proses untuk menentukan apakah suatu proses adalah *malware* atau bukan. Dari hasil penelitian mengenai sistem pendeteksian *malware*, dapat disimpulkan bahwa dapat mendeteksi *malware* dengan menggunakan analisis dinamis. Program pendeteksi malware yang dibuat sudah memenuhi tujuan dari penelitian yang dilakukan yaitu membuat aplikasi yang dapat mendeteksi *malware* di komputer dan mengirimkan data tentang aktifitas *malware* yang terjadi di komputer.

Kata-kata kunci: malware, analisis dinamis, virus, worm, trojan

ABSTRACT

Nowadays, usage of computers, notebook and its kind is increasing. There is a lot of operating system that used by those hardware, for example Ubuntu, Debian and Windows. Right now the one who most used by people in the world is Windows operating system. In Windows operating system, there is a lot of application that can be used to help a certain activity. For example is word processor, web browser and spreadsheet processor. Sometimes, there is a harmful software that doing harmful activities that compromising running system. Those activities is hidden so when the application making any changes, the changes won't be noticed by user. Usually the kind of harmful software detector did nott make any log for what that has been changed by those applications. The hidden activities usually is editing a file, copying a file, deleting a file, sending a file via network and accessing network or website without user consent. Even tough those activities are considered normal, those activity can be dangerous if the activities said before was done without user noticing and the files used in those activities is a system file or users important file. There is a chance that the harmful application will access harmful websites and networks, for example the sites where when accessed will download malware to the system right away.

The point of this research is to make an application that can log malwares activities to system, and sending its log to the server about the malwares activities that has been done in that computer. With the logs user will be known about the attack done by malware.

Dynamic analisis is an analysis that using a proses behavior to deduce, is the proses is a malware or not. From the research about malware detection system, can be deducted that in analysis stage that we can use dynamic analysis to detect malware. Activity detector application that has been made is fulfilling this research point, that is making an application that can detect malware activity and sending log to server about the malware activity at the computer

Keywords: malware, dynamic analysis, virus, worm, trojan

keluargaku

KATA PENGANTAR

Puji dan syukur kepada Tugan Yang Maha Esa atas segala kelimpahan rahmat, berkat dan bimbingan-Nya sehingga penulis dapat menyelesaikan skripsi ini sesuai dengan waktu yang telah direncanakan. Penulis menyadari bahwa di dalam skripsi ini masih terdapat kekurangan-kekurangan yang disebabkan terbatasnya kemampuan dan pengetahuan yang dimiliki penulis. Pada kesempatan ini, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Orang tua penulis yaitu Juniarto dan Nenden, yang selalu memberikan dukungan selama penulis mengerjakan skripsi ini.
2. Bapak Chandra Wijaya selaku dosen pembimbing yang telah memberikan banyak bantuan berupa kritik, saran dan nasihat dalam penyusunan skripsi ini.
3. Para Administrator Laboratorium FTIS, yaitu Eca, Kalas, Ncen, Gun dan Sam sebagai teman yang selalu membantu penulis baik dalam penulisan skripsi atau dalam kehidupan sehari-hari.
4. Takenaka Mayu yang selalu memberikan semangat kepada penulis saat penulisan skripsi ini.
5. Rekan-rekan Teknik Informatika 2013 yang tidak bisa disebutkan satu-per-satu.
6. Laptop pribadi penulis yang telah setia menemani penulis dalam keadaan apapun.

Akhir kata penulis berterima kasih dan memohon maaf kepada pihak-pihak yang telah membantu tetapi tidak tertuliskan oleh penulis. Kesempurnaan hanyalah milik Tuhan semata, oleh karena itu penulis dengan sepenuh hati akan menerima kritik dan saran yang dapat membantu penyempurnaan skripsi ini.

Bandung, Mei 2017

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1

PENDAHULUAN

Pada bagian ini akan dijelaskan tentang latar belakang pengambilan judul skripsi ini, masalah yang dihadapi, batasan masalah, tujuan dari skripsi ini, metodologi penelitian dan sistematika penelitian dari skripsi ini.

1.1 Latar Belakang

Pada masa kini, pemakaian komputer dan notebook sudah sangat banyak. Ada banyak sistem operasi yang digunakan oleh perangkat-perangkat tersebut, contohnya adalah Ubuntu, Debian, dan Windows. Saat ini yang paling umum digunakan di dunia ini adalah sistem operasi Windows. Pada sistem operasi Windows, banyak aplikasi yang dapat digunakan untuk membantu aktivitas tertentu. Contohnya adalah aplikasi pengolah kata, peramban internet, dan pengolah data. Terkadang, ada aplikasi berbahaya yang melakukan aktivitas-aktivitas yang membahayakan sistem yang berjalan. aktivitas yang dilakukan oleh aplikasi tersebut bersifat tersembunyi sehingga jika aplikasi tersebut melakukan suatu perubahan, perubahan tersebut tidak terdeteksi oleh pengguna. Biasanya, perangkat lunak yang mendeteksi ini tidak menyimpan data perubahan apa saja yang dilakukan oleh aktivitas tersembunyi tersebut. aktivitas tersembunyi biasanya adalah mengubah sebuah *file*, menduplikasi *file*, menghapus *file*, mengirim *file* melalui jaringan, mengakses jaringan tertentu atau situs tertentu. Walaupun aktivitas-aktivitas tersebut merupakan hal yang normal, aktivitas tersebut bisa menjadi berbahaya jika aktivitas-aktivitas yang disebutkan di atas dilakukan tanpa sepengetahuan pengguna dan *file* yang digunakan oleh aktivitas tersebut merupakan *file* sistem atau *file* penting milik pengguna. Ada kemungkinan juga aplikasi yang berbahaya itu akan mengakses situs-situs atau jaringan yang berbahaya, misalnya situs-situs yang ketika diakses akan mengunduh *malware*.

Semua perangkat lunak yang melakukan aktivitas berbahaya di suatu sistem disebut dengan *malware*[1]. *Malware* adalah singkatan dari *Malicious Software*, yaitu perangkat lunak yang jika aktif dapat merusak kerja perangkat, mengumpulkan data-data sensitif, mendapatkan akses ke perangkat target atau menampilkan iklan yang menganggu[1]. *Malware* dapat muncul dengan berbagai bentuk seperti berkas *executable*, *scripts* dan konten aktif seperti *flash*. Salah satu contoh *malware* yang terkenal adalah *Sony Rootkit*. *Sony Rootkit* adalah *malware* yang dipasang oleh Sony di dalam CD yang dijual yang kemudian jika dipakai oleh pembeli akan secara otomatis dipasang di perangkat pengguna agar mencegah pembajakan lagu. Tetapi secara tidak langsung *malware* ini juga menyadap aktivitas pengguna dan juga membuat celah yang dapat digunakan oleh *malware* lain untuk menyerang perangkat korban. Kurang sadarnya para pengguna komputer menyebabkan *malware* mudah untuk menyebar. Penyebaran *malware* terjadi dengan banyak cara, seperti menyisipkannya di program yang korban unduh, melalui *flashdisk*, dan melalui dokumen dengan cara menyisipkan kode program di dokumen tersebut.

Pada saat ini banyak perusahaan yang sudah membangun *anti-malware*. *Anti-malware* adalah aplikasi yang digunakan untuk mendeteksi malware. Teknik yang digunakan oleh *anti-malware* juga ada dua macam, yaitu statis dan dinamis. Teknik analisis statis hanya akan mengecek *malware* dari isi berkas saja sedangkan teknik analisis dinamis akan mengecek *malware* dari aktivitas yang

dilakukan suatu proses. Teknik analisis dinamis akan mengandalkan *hook* ke sebuah proses agar dapat menganalisis apa yang dilakukan oleh suatu proses. Pendeteksian oleh *anti-malware* pada saat ini hanya mendeteksi file yang terinfeksi tanpa adanya informasi tentang perubahan apa saja yang telah dilakukan oleh *Malware*. Sehingga pengguna tidak mengetahui apakah *malware* telah menghapus berkas milik pengguna atau mengubah berkas milik pengguna. Dengan adanya aplikasi pendeteksi *malware* yang mencatat aktivitas *malware*, maka jika ada aktivitas yang mencurigakan dapat memberitahukan ke korban, yang kemudian dapat dilakukan perbaikan atau pencegahan terhadap *malware* sebelum terjadi kerusakan yang lebih parah.

1.2 Rumusan Masalah

- Bagaimana cara mendeteksi *malware* yang melakukan aktivitas yang berbahaya
- Bagaimana cara merekam aktivitas dari suatu *malware*
- Bagaimana cara mengirim catatan yang telah direkam ke server yang ada

1.3 Tujuan

Tujuan dari penelitian yang dibuat adalah untuk membuat aplikasi yang dapat mencatat aktivitas *malware* di dalam suatu sistem, dan mencegah *malware* tersebut aktif. Selain mendeteksi dan mencegah aktivitas *malware* di dalam suatu siste, akan mencatat aktivitas tersebut dan mengirimkan catatan tersebut ke server yang dibangun.

1.4 Batasan Masalah

Batasan masalah yang digunakan saat menulis skripsi ini adalah:

1. *Malware* yang diambil untuk analisis dan percobaan adalah *malware* yang berupa file *executable*.
2. Sistem operasi yang digunakan adalah Windows 7 64-bit.

1.5 Metodologi Penelitian

Langkah-langkah yang dilakukan dalam skripsi ini adalah:

1. Studi Pustaka
   Tahap ini dilakukan untuk memahami pengetahuan mengenai dasar-dasar teori yang berhubungan dengan pendeteksian *malware*, dan juga mengetahui cara komunikasi antara klien dan *server*.
2. Menganalisis dan merancang Program
   Tahap ini dilakukan untuk merancang program yang akan dibuat sesuai dengan kebutuhan sistem. Perancangan yang dilakukan termasuk dengan perancangan *database* untuk pelaporan aktivitas dan sistem pendeteksi *malware*.
3. Mengimplementasikan Perangkat Lunak1
   Tahap ini dilakukan untuk mengimplementasikan perangkat lunak Aplikasi Pendeteksi Aktivitas Komputer Tersembunyi.
4. Melakukan Pengujian Terhadap Perangkat Lunak
   Tahap ini dilakukan untuk menguji perangkat lunak yang telah dibuat, menguji kesesuaian perangkat lunak dengan tujuan skripsi atau tidak.

5. Penarikan Kesimpulan
   Tahap ini dilakukan untuk mengambil kesimpulan berdasarkan pengujian yang telah dilakukan.

1.6 Sistematika Pembahasan

Sistematika pembahasan penelitian ini, yaitu:

1. Bab 1 Pendahuluan, berisi mengenai permasalahan yang akan dibahas dalam penelitian yang akan dilakukan dan mejelaskan latar belakang, rumusan masalah, tujuan, metodologi beserta sistematika pembahasan.

2. Bab 2 Dasar Teori, berisi mengenai pengetahuan dan teori dasar mengenai *Malware* dan jenisnya, kemudian juga tentang *System Call*, cara pendeteksian *malware*, *library* Deviare2, IDE (Integrated Development Environment) Visual Studio, dan tentang Sistem Operasi.

3. Bab 3 Analisis, berisi hasil analisis terhadap masalah dan juga kebutuhan aplikasi yang akan dibangun, sebagai jawaban permasalahan yang dihadapi saat ini.

4. Bab 4 Perancangan, berisi rancangan untuk program yang dibangun, mulai dari kelas diagrams sampai dengan algoritma yang dimiki setiap fungsi

5. Bab 5 Implementasi dan Pengujian, berisikan hasil implementasi dan hasil pengujian dari program yang telah dibangun

6. Bab 6 Kesimpulan dan Saran, berisikan kesimpulan yang bisa ditarik dari masalah ini dan saran yang bisa diberikan.