IMPLEMENTASI METODE PENCARIAN (*HSC) HEADER SIZE OF CODE* DAN TITIK MASUKAN PENGALAMATAN PADA RANCANGAN SOFTWARE ANTI VIRUS

Nurul Chafid[1], Rizky Tsaunauval Braselino[2]
Program Studi Teknik Informatika Fakultas Teknik
Dosen Fakultas Teknik[1], Mahasiswa Fakultas Teknik[2]
Universitas Satya Negara Indonesia
Email: chafid09@gmail.com[1]

ABSTRAK

Virus merupakan penyakit menular yang menjadi sebuah ancaman bagi sekian banyak jenis alat elektronik khususnya perangkat komputer dan laptop, serta pocket PC yang disinyalir virus tersebut menyerang melalui jaringan internet dan berbagai media penyimpanan yang di salurkan melalui konektor lewat flash disk atau penyimpanan lainnya.

Teknik kerja anti-virus dapat membuat pencarian file data yang terheader mendeteksi ukuran file yang sangat kecil serta berbagai macam file dan berasal dari kode dan masuknya titik masuk posisi dimana file akan terjangkit dan bisa terjadi kerusakan. Namun anti virus ini tidak menggunakan algoritma matematika, anti virus ini menggunakan program algoritma yang artinya hanya menunjukkan aliran dari sistem yang dijalankan, ketika diklik oleh pengguna akan mendeteksi dalam hal ini anti virus bekerja dengan memindai setiap file dan mencocokkannya dengan tanda tangan virus yang dimilikinya dengan membuat duplikat sebelumnya. tanda tangan virus mengandung hexa desimal yang memiliki 32 karakter.

Penelitian ini bertujuan untuk: (1) menentukan perilaku virus dan bakteri. (2) mendesain anti virus itu sendiri. Berdasarkan penelitian di atas disimpulkan bahwa rancangan Anti-virus menggunakan alamat entri dan Ukuran Kode sebagai pola dari virus ini, juga dapat diandalkan sebagai mesin pemindai, yang dapat diandalkan untuk mengidentifikasi virus, dan juga efisien. dalam penggunaan memori recource.

Kata Kunci: Anti Virus, File PE, Alamat Titik Masuk Dan Ukuran Kode.

ABSTRACT

A virus is an infection disease that is a threat to many types of electronic devices, especially computer devices and laptops, as well a pocket PC which are allegedly attacked by the internet and various storage media that are channeled through connectors via flash disks or other storage.

The anti-virus working technique can make the search data file that is detected by detecting a very small file size and various kinds of files and comes from the code and the entry of the entry point where the file will be infected and damage can occur. But this anti virus does not use mathematical algorithms, this anti virus uses an algorithm program which means it only shows the flow of the system being run, when clicked by the user it will detect in this case the anti virus works by scanning each file and matching it with the virus signature it has duplicate before. signature of a heximal decimal containing 32 characters.

This study aims to: (1) determine the behavior of viruses and bacteria. (2) designing the anti virus itself. Based on the above research it can be concluded that the Anti-virus design uses the address entry and Code Size as a pattern of this virus, can also be relied on as a scanning machine, which can be relied upon to identify viruses, and also be efficient. in recource memory usage.

Keywords: *Anti Virus, PE Files, Address Entry Points and Code Size*

PENDAHULUAN

Dewasa ini kemajuan teknologi informasi khususnya di bidang teknologi computer berkembang dengan sangat pesat, sebanding dengan kemajuan teknologi yang sangat pesat hal ini berpengaruh terhadap keamanan dan isu yang kerap kali dibahas. Mulai dari ancaman langsung para craker atau hacker jahat hingga acaman yang dilakukan melalui program yang disebut malcode (malicious code). Suatu program atau script apapun yang bersifat merusak atau merugikan dapat katagorikan sebagai malcode termasuk virus komputer, worm atau trojan horse.

Selama lebih dari 20 tahun terakhir,virus komputer telah berkembang dari sekedar riset akademis menjadi masalah yang umum bagi para pengguna komputer di dunia. Masalah terbesar dari virus ini berasal dari penanggulangan efek kerugian yang ditimbulkan oleh penyebarannya. Efek kerugian ini semakin menjadi dengan maraknya penggunaan internet sebagai jalur komunikasi global antara pengguna komputer di seluruh dunia. Berdasarkan hasil survei CSI/FB sejak tahun 1999-2006 pada sekitar 300-an responden dari berbagai organisasi di Amerika Serikat, tentang kejahatan komputer dan keamanannya, menyebutkan bahwa virus menempati urutan pertama sebagai kejahatan komputer yang paling merugikan. Masih dari hasil survei tersebut, dinyatakan kerugian rata-rata yang diderita organisasi-organisasi itu akibat virus komputer ditaksir mencapai sekitar 38 juta dolar amerika pertahun. Seiring dengan perkembangannya, virus komputer mengalami beberapa evolusi dalam bentuk, karakteristik serta media penyebarannya. bentuk evolusi tersebut dikenal dengan Worms, Spyware, Trojan horse dan program Malcode lain. Perkembangan penyebaran malcode di Indonesia pada awalnya lebih banyak didominasi oleh worms dan virus yang berasal dari luar negeri. Namun pada bulan Oktober 2005, dominasi ini mulai runtuh dengan menyebarnya virus-virus lokal yang hampir ada disetiap komputer di seluruh Indonesia, virus menyebar dengan sangat cepat dan membuat masalah bagi pengguna komputer, dengan demikian dibuatlah anti virus sebagai salah satu solusi mencegah penyebaran.

Metode pencarian virus yang paling sering di pakai oleh anti virus yaitu metode CRC-32 (Cyclic Redundancy Code). Metode CRC-32 merupakan teknik yang semulanya digunakan untuk mengecek kerusakan pada file. Metode ini yang sering digunakan oleh anti virus lokal untuk mengecek signature dari virus. Kasus virus lokal sudah ditemukan penggunaan teknik polymorph. Baik itu secara sederhana maupun kompleks. Hal ini yang melatarbelakangi mengapa "Metode Pencarian Header Data Size Of Code Dan Address Of Entry Point Pada Desain Anti Virus" diangkat sebagai judul skripsi. Berdasarkan pengamatan penulis setelah penulis teliti walau virus sudah melakukan modifikasi size pada dos header tetapi data optimal header dari virus yang berupa *Size Of Code* dan titik masukan pengalamatan tidak akan berubah.

TINJAUAN PUSTAKA

Dalam melengkapi penelitian ini, penulis mengambil sumber pustaka dari salah satu jurnal ilmiah berjudul "Aplikasi Pengekstrak Pola Dan Pendeteksi Worms Dengan Pendekatan Pelacakan Entry Point" yang ditulis oleh Hendra S.T., M.T (2011) dan Matt

Pietrek (2002), "*Inside Windows : An InDepth Look into the Win32 Portable Executable File"*. Dalam penjelasannya mengenai virus komputer dimana virus komputer itu memiliki ciri khas yang digambarkan sebagai pattern sedangkan aslinya virus dilacak dengan cara memindai registry,startup program, sevices, process, dan lain-lain. PE file juga memiliki pernanan pernting dalam pendeteksian virus, PE file merujuk ke entry point dari virus. Sehingga virus juga dapat dideteksi dengan melihar *Size Of Code* dan *Address Of Entry Pointnya*.

Dalam Jurnal penelitian yang ditulis oleh Richki Hardi penjelasannya mengatakan bahwa Era globalisasi adalah termasuk era dimana virus komputer telah berkembang pesat,tidak hanya dari sekedar riset akademis melainkan sudah menjadi masalah umum bagi para pengguna komputer di dunia. Efek kerugian ini semakin menjadi dengan maraknya penggunaan internet sebagai jalur komunikasi global antara pengguna komputer di seluruh dunia, berdasarkan hasil survei CSI/FB. Seiring dengan perkembangannya, virus komputer mengalami beberapa evolusi dalam bentuk, karakteristik serta media penyebarannya seperti Worms, Spyware, Trojan horse dan program Malcodelain. Melalui Pengembangan antivirus berbasis clien server maka user dapat dengan mudah mengetahui tingkah laku dari virus dan worm, mengetahui bagian apa saja dari sebuah sistem operasi yang diserang oleh virus dan worm, membuat sebuah pengembangan antivirus sendiri berbasis jaringan client server serta dapat juga diandalkan sebagai sebuah engine scanner yang cepat dan handal untuk mengenali virus dan hemat dalam manajemen memori.(Jurnal Telematika, Vol.12,No.2, Juli 2015;p.82-98)

LANDASAN TEORI

Pengertian Virus Komputer

Istilah virus komputer tak asing lagi bagi kalangan pengguna komputer saat ini. Padahal, sekitar 12 tahun yang lalu, istilah ini telah dikenal oleh masyarakat pengguna komputer. Baru pada tahun 1988, muncul artikel-artikel di media massa yang dengan gencar memberitakan mengenai ancaman baru bagi para pemakai komputer yang kemudian dikenal dengan sebutan 'virus komputer'. Virus yang terdapat pada komputer hanyalah berupa program biasa, sebagaimana layaknya program-program lain. Tetapi terdapat perbedaan yang sangat mendasar pada virus komputer dan program lainnya.Virus dibuat oleh seseorang dengan tujuan yang bermacam-macam, tetapi umumnya para pembuat virus hanyalah ingin mengejar popularitas dan juga hanya demi kesenangan semata. Tetapi apabila seseorang membuat virus dengan tujuan merusak maka tentu saja akan mengacaukan komputer yang ditularinya.

Kemampuan Dasar Virus

Umumnya virus komputer adalah program komputer yang biasanya berukuran kecil yang dapat menyebabkan gangguan atau kerusakan pada sistem komputer dan memiliki beberapa kemampuan dasar, diantaranya adalah :

- Kemampuan untuk memperbanyak diri
  Yakni kemampuan untuk membuat duplikat dirinya pada file-file atau disk-disk yang belum ditularinya, sehingga lama-kelamaan wilayah penyebarannya semakin luas.
- Kemampuan untuk menyembunyikan diri.
  Yakni kemampuan untuk menyembunyikan dirinya dari perhatian user, antara lain dengan cara-cara berikut :
  a) Menghadang keluaran ke layar selama virus bekerja, sehingga pekerjaan virus tak tampak oleh user.

b) Program virus ditempatkan diluar track2 yang dibuat DOS .
c) Ukuran virus dibuat sekecil mungkin sehingga tidak menarik kecurigaan.

- Kemampuan untuk mengadakan manipulasi
  Sebenarnya rutin manipulasi tak terlalu penting. Tetapi inilah yang sering mengganggu. Biasanya rutin ini dibuat untuk :
  a). Membuat tampilan atau pesan yang menggangu pada layar monitor
  b). Mengganti volume label disket
  c). Merusak struktur disk, menghapus file-file
  d). Mengacaukan kerja alat-alat I/O, seperti keyboard dan printer
- Kemampuan mendapatkan informasi
  Yakni kemampuan untuk mendapatkan informasi tentang struktur media penyimpanan seperti letak boot record asli, letak tabel partisi, letak FAT32, posisi suatu file, dan sebagainya.
- Kemampuan untuk memeriksa keadaan dirinya
  Sebelum menyusupi suatu file, virus akan memeriksa keberadaan dirinya di dalam file tersebut dengan mencari ID (tanda pengenal) dirinya. File yang belum tertular suatu virus tentunya tidak mengandung ID dari virus yang bersangkutan. Kemampuan ini mencegah penyusupan yang berkali-kali pada suatu file yang sama.

Penyebaran Internet

Akhir-akhir ini virus yang menyebar dengan media sudah semakin banyak, virus ini biasanya menyebar lewat e-mail ataupun pada saat user mendownload suatu file yang mengandung virus. Juga ada beberapa virus yang secara otomatis akan menyebarkan dirinya lewat e-mail apabila komputer memiliki hubungan ke jalur internet.

Sejarah Singkat Antivirus

Sebagian besar dari virus komputer yang ditulis pada tahun 1980 awal dan pertengahan terbatas pada diri-reproduksi dan tidak memiliki rutinitas kerusakan khusus dibangun ke kode. Itu berubah ketika programmer lebih banyak berkenalan dengan pemrograman virus dan menciptakan virus yang dimanipulasi atau bahkan menghancurkan data pada komputer yang terinfeksi.Ada klaim bersaing untuk inovator produk antivirus pertama. Mungkin penghapusan didokumentasikan publik pertama dari virus komputer di alam liar dilakukan oleh Bernd Fix pada tahun 1987.

Fred Cohen, yang menerbitkan salah satu koran akademis pertama mengenai virus komputer pada tahun 1984, mulai mengembangkan strategi untuk perangkat lunak antivirus pada tahun 1988 yang dijemput dan dilanjutkan oleh pengembang perangkat lunak kemudian antivirus.

Juga pada tahun 1988 sebuah milis bernama VIRUS-L dimulai pada jaringan / BITNET EARN mana virus baru dan kemungkinan mendeteksi dan menghilangkan virus telah dibahas. Beberapa anggota milis ini seperti John McAfee atau Eugene Kaspersky kemudian mendirikan perusahaan perangkat lunak yang dikembangkan dan menjual perangkat lunak antivirus komersial. Sebelum konektivitas internet tersebar luas, virus yang biasanya disebarkan melalui disket yang terinfeksi. Perangkat lunak antivirus mulai digunakan, tetapi telah diupdate relatif jarang. Selama waktu ini, pada dasarnya virus checkers harus memeriksa file yang dapat dieksekusi dan sektor boot dari floppy disk dan

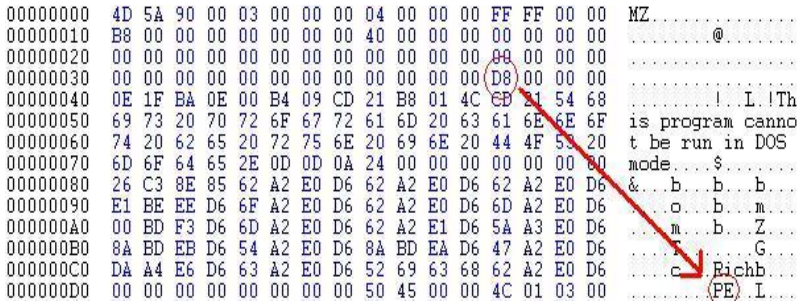
hard disk. Namun, seperti penggunaan internet menjadi umum, akhirnya virus mulai menyebar di dunia maya.

Header File (PE)

Format File PE (Portable Executable) mulai dikenalkan pada Windows NT 3.1, dimana format file ini masih menyimpan header MZ dari MS-DOS. Berikut beberapa bentuk struktur dari PE:

a. Struktur File (Portable Executable)

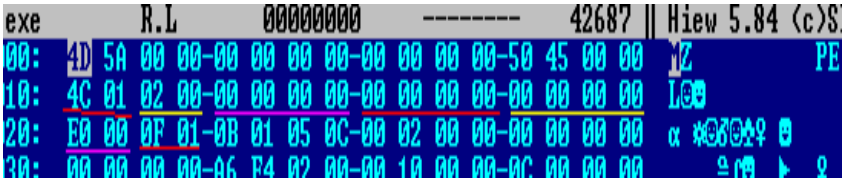
Suatu file PE akan diawali dengan suatu DOS Header yang memiliki suatu e_magic number dalam hexa 4D 5A (MZ, lihat gambar dibawah), kemudian pada offset ke 60 atau hexa D8 akan terdapat suatu pointer (e_lfanew) yang menunjuk kelokasi dimana PE file header. Berikut gambar dari struktur file PE:



Gambar 1. DOS Header dari PE File

b. PE Header

PE Header merupakan salah satu struktur dari IMAGE_NT_HEADER (dideklarasikan dalam WIN NT.H). Header ini mengandung berbagai macam jenis informasi seperti lokasi dan ukuran dari area kode dan data, sistem operasi yang dipakai, ukuran stack, dan lain-lain. Header ini juga mengandung MS-DOS stub, yaitu program kecil yang akan menampilkan teks "This program cannot be run in MS-DOS mode. Maka ketika dijalankan maka akan muncul seperti pada gambar berikut:



Gambar 2. Data Image File Header

METODE PENELITIAN

Teknik Penyiapan Pattern Virus

Langkah pertama dari pembuatan program antivirus adalah memiliki pattern atau virus yang akan dikenali oleh program antivirus. Pattern bisa juga disebut pola atau susunan. Sebuah program antivirus tidak akan bermanfaat jika tidak didukung oleh virus definition yang lengkap, definition file adalah suatu kumpulan data dari malicious code. Jadi industri antivirus sangat tergantung dari dukungan sample virus yang dikirim kepada mereka.

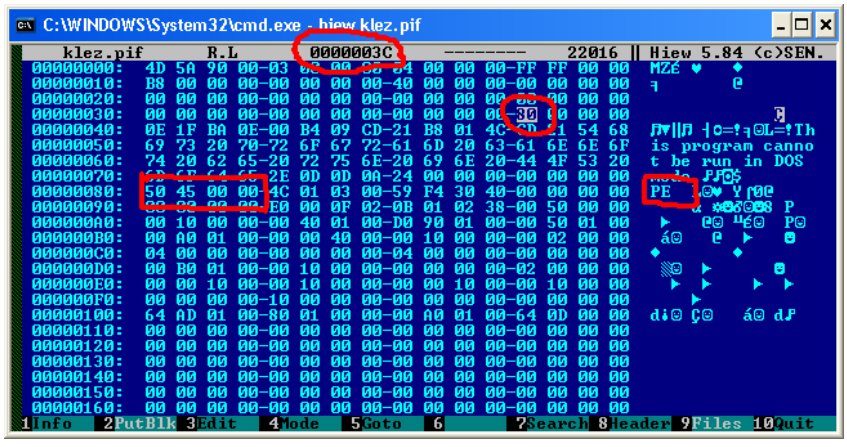
Walaupun dewasa ini telah dilakukan berbagai pendekatan heuristic dalam pendeteksian program-program virus, tetapi hal tersebut sering tidak efektif karena akan membuat system menjadi rewel dan sering memberikan false alarm dimana program-program utility tert entu dianggap sebagai virus, oleh karena itu pembuat virus telah memperbaiki teknik pengkodean sehingga dapat memperdaya program-program antivirus.

Tentu saja hal ini membutuhkan penelitian dan analisa yang mendalam sehingga teknik pengumpulan pattern virus menjadi efektif untuk mendeteksi keberadaan process virus dimemori maupun file virus dimedia penyimpanan. Masalah lain adalah teknik penyiapan pattern virus akan mempengaruhi teknik pendeteksian yang tentu saja sangat menentukan performance dari antivirus yang dibuat, misalnya pattern virus telah berkembang menjadi 100 pattern dan jumlah file yang akan dideteksi adalah 1000 files, sehingga dilakukan perkalian menjadi 100000 kali proses pendeteksian, bagaimana kalau pattern berkembang menjadi 1000, dan terakhir adalah resource yang digunakan untuk penyimpanan pattern tersebut baik media disk maupun memori. Jadi teknik pembuatan pattern virus merupakan isu yang terpenting dari kesuksesan pendeteksian program antivirus dan perfomancenya, serta resource yang dihabiskan. Ini merupakan bagian yang paling penting dari suatu program antivirus. Karena bagaimana pattern virus tersebut dilakukan (mengambil pattern dari file virus), maka dengan cara sebaliknya program anti virus akan mendeteksi keberadaan virus file dan process virus dimemori (dengan membandingkan pattern virus dengan data file dan process).

Teknik pendekatan yang digunakan penulis merupakan hasil pengamatan dan penelitian terhadap beberapa program virus yang beredar di Indonesia, seperti varian Brontok dan MyHeart. Pendekatan ini cukup efektif untuk digunakan untuk mengenali keberadaan process virus di memori maupun di file dengan satu pendekatan yang sama.

Dos *Header* Pada Beberapa Virus

Pada PE file standard dapat dengan mudah mendapatkan posisi PE Header, dengan mengambil pointer e_lfanew. Tetapi pada beberapa virus hal tersebut tidak dapat dilakukan, karena mereka telah melakukan modifikasi terhadap DOS Header dengan tujuan mereduksi ukuran dari program Virus. Contoh DOS Header pada Worm Klez yang masih standar. di perlihatkan pada gambar berikut.



Gambar 3. Dos Header

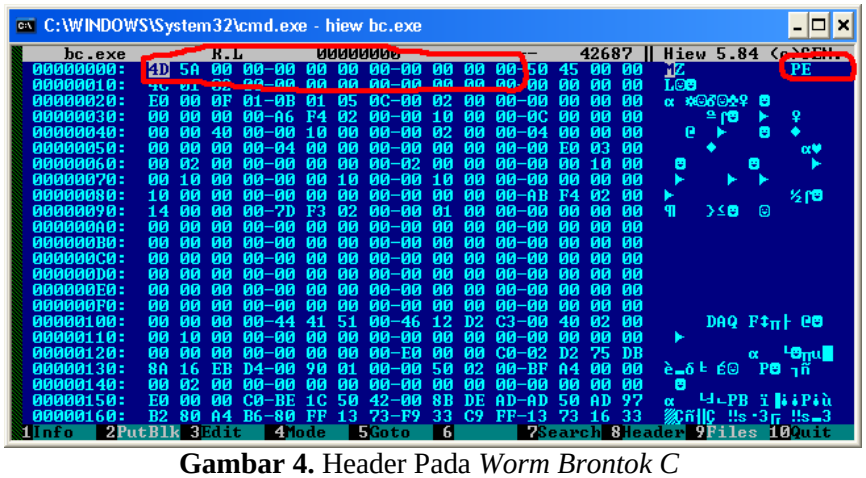
Keterangan Gambar

Dimana pada offset 3C hexa (e_lfanew) berisi nilai 80 hexa yang merupakan pointer ke lokasi dimana PE header berada, yaitu pada posisi Offset 80 hexa, kalau dilihat pada

gambar diatas berisi nilai 50 45 hexa yang merupakan representasi dari nilai ASCII P (50 hexa) dan E (45 hexa).

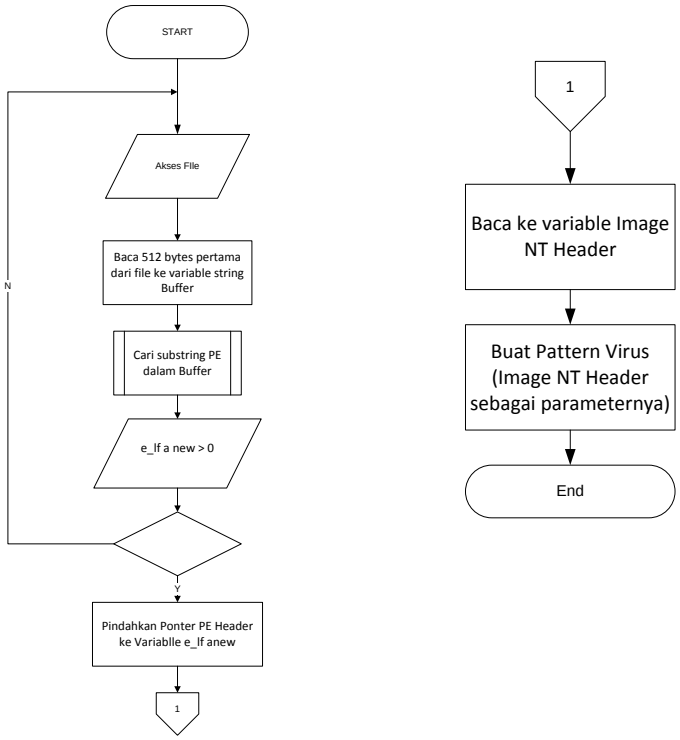
Fakta DOS *Header* Pada *Worm* Brontok C

Berdasarkan pengamatan penulis, ternyata pembuat virus telah melakukan modifikasi terhadap PE file dengan mereduksi DOS Header.



Gambar 4. Header Pada *Worm Brontok C*

Pada gambar diatas tidak dapat menggunakan pendekatan sebelumnya untuk menentukan posisi PE header, sehingga perlu dilakukan dengan cara pencarian data “PE”+Chr$(0)+Chr$(0) pada buffer pembacaan file, e_lfanew = InStr(sBuffer, "PE" + Chr$(0) + Chr$(0). Berikut flowcart proses dalam kinerja header WBC.



Gambar 5. Flowcart Teknik Penyiapan Pattern Virus

HASILDAN PEMBAHASAN

Menyimpan Pattern Virus Ke Prorgam

Kita langsung memasukkan pattern virus kedalam program, tetapi tentu saja pendekatan ini tidak efektif, dimana setiap ada pattern baru, maka harus melakukan modifikasi terhadap source code dan melakukan kompilasi ulang, kedepannya akan ditambahkan menu penyimpanan pattern virus di file terpisah. Diawali dari nama virus dan diikuti oleh 32 digit pola virus yang berupa bilangan hexa. Sehingga :

Nama Virus Pattern Virus

XXXXXXXXXXXX;yyyyyyyyyyyyy

a). W31 SALITY; 1300FB1541C783D042B41B2EA2C1F96E

b). W32 WORM/GEN; 7CDC6C21D92AF00E071D72A9496703B0

c). TROJAN GEN; F97F4EE2096578C592D30367177BCCC3

d). WIN32 TROJAN HORSE; 754A9DD982DA023AEA6E1D7A711BC724

e). Dst.

Setiap startup program antivirus cukup membaca semua pattern tersebut ke suatu variable array.

Dim PatternCount As Integer

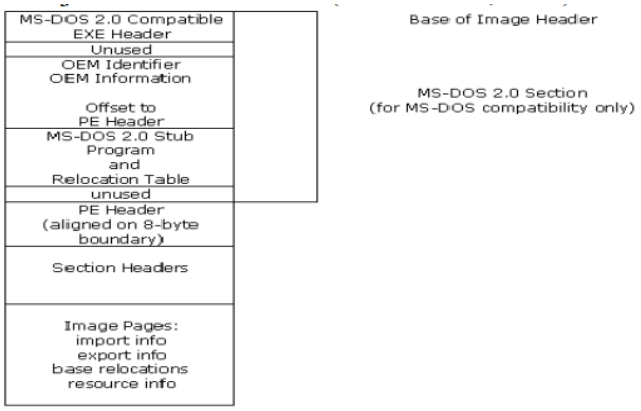
Dim PatternVirus(100) As String

Pembuatan Cheksum Menggunakan PE

PE (*Portable Executable*) sendiri mempunyai struktur data yang tersusun dan tertata rapi baik secara fisik maupun virtual (di memory) sehingga dapat kita baca data-datanya dengan baik .Dalam pembuatan antivirus PE sangatlah penting karena virus pasti menginfeksi file-file program yang tergolong jenis file PE satu ke file PE yang lain. Adapun data yang akan kita kalkulasi adalah sebagai berikut:

- *Time Date Stamp* : Data tanggal compilasi PE.
- Characteristics pada Image File Header : Pembeda antara PE jenis data exe , dll data *sys*.
- *Address Of Entry Point ; Relative virtual address* dari file PE.

Untuk menjelaskan bagaimana teknik pengambilan pola yang dikembangkan oleh penulis, maka berikut ini akan dilakukan tinjauan terhadap struktur file program worms. Sebagaimana program executable lainnya, struktur file worms pada juga menggunakan format *Portable executable* (PE). PE adalah format dari program-program *binary (exe, dll, sys, scr)* untuk MS *windows* NT, windows 95 dan Win32s. Suatu PE file terdiri dari beberapa bagian informasi yang ditunjukan oleh Gambar 1. (Matt Pietrek, 2002).



Gambar 6. Struktur File PE

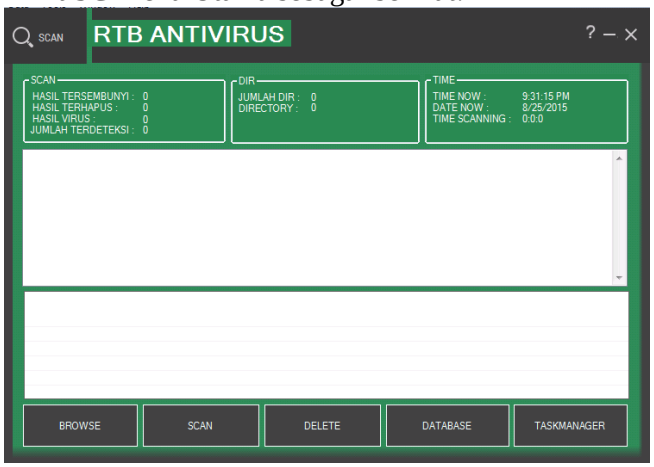
PE File Section

Sections mengandung isi dari file, termasuk kode, data dan resource, dan informasi executable lainnya. Masing-masing section memiliki suatu header dan satu body (the raw data). Section header berada pada posisi setelah PE Optional header. Masing-masing header memiliki struktur yang berukuran 40 byte, berikut ini adalah section header yang dinyatakan sebagai struktur data C.

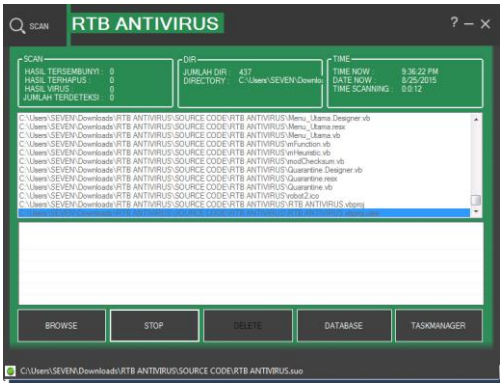
Public Signature As Long
'Public FileHeader As IMAGE_FILE_HEADER
'Public OptionalHeader As IMAGE_OPTIONAL_HEADER
'Public OptionalHeaderNT As IMAGE_OPTIONAL_HEADER_NT
Public Machine As Integer
Public NumberOfSections As Integer
Public TimeDateStamp As Long
Public PointerToSymbolTable As Long
Public NumberOfSymbols As Long
Public SizeOfOptionalHeader As Integer
Public Characteristics As Integer

Implementasi Antivirus

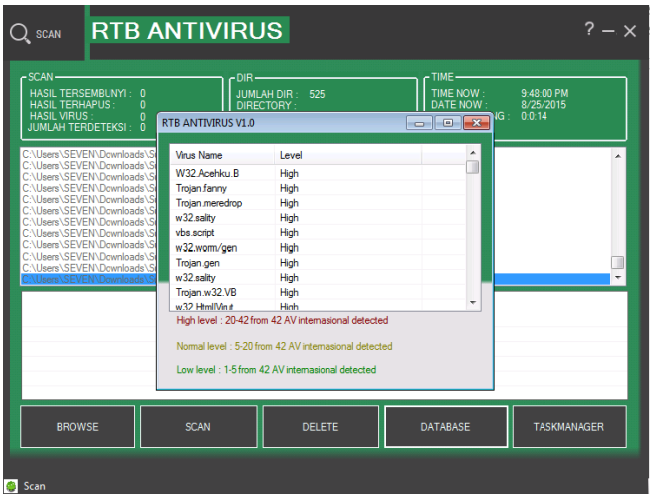
Berikut adalah tampilang jalannya aplikasi, dengan perangkat yang dibuat menggunakan Print SC Menu Utama sebagai berikut:



Pada menu tampilan ini berisi menu browse, scan, delete, database dan *Task Manager* , masing masing berfungsi untuk melakukan scan virus, menghapus file , melihat database virus dan melihat *Task Manager*.



Gambar diatas menunjukan loading bar proses scan aplikasi saat berjalan, disini dilengkapi pula dengan menu stop jika user menginginkan. Berikut list Virus yang terdeteksi dalam database:



KESIMPULAN DAN SARAN

Kesimpulan

Dari hasil teknik uji coba dari sistem anti virus ini dapat di ambil kesimpulan bahwa:

a) Teknik penggunaan header file address of entry point dan size of code cukup akurat dalam mengenal virus walau sudah merubah header filenya tapi datanya masih sama.
b) Sebagaimana file executable Windows biasanya, program Worms komputer memiliki struktur PE file, tetapi tidak tertutup kemungkinan terjadi reduksi pada DOS header.Kunci utama pendeteksian virus komputer adalah ketersediaan signature unik yang digunakan sebagai pola pendeteksian.Pengambilan beberapa byte awal executable virus pada posisi entry point dapat dijadikan sebagai signature untuk mendeteksi worms tersebut.
c) Telah berhasil membuat anti virus dengan metode pencarian virus signature (pattern virus) menggunakan pendekatan size of code dan address of entry point (titik masukan pengalamatan).

Saran

Virus ini juga perlu di tingkatkan sensitifitasnya, karena bila terdapat section dummy pada urutan section kedua atau tidak ada pada section, atau pembelokan pada entry pointnya maka data yang di teliti bisa saja salah, Fungsi ini juga masih rawan dari kesalahan analisa. Lamanya proses scan virus juga menjadi kekurangan dari anti virus ini. Anti virus ini juga masih terbatas hanya membaca path file belum ke registry dan sebagaiannya. Database juga harus diperbanyak karena 100 database saja masih jauh dari cukup. Maka dari itulah butuh penelitian lebih lanjut, agar dapat mengembangkan dan memajukan kualitas aplikasi anti virus..

DAFTAR PUSTAKA

Aat Shadewa, 2006, Rahasia Membuat Anti virus Menggunakan Visual Basic, Yogyakarta: Penerbit DSI Publishing

Gordon, A., Lawrence et. al., (2006), CSI/FBI Computer Crime and Security Survey 2006, CSI Publication, Washington DC, http://www.GoCSI.com/, 1 November 2006.

Hendra S.T., M.T (2011) "Aplikasi Pengekstrak Pola Dan Pendeteksi Worms Dengan Pendekatan Pelacakan Entry Point"

Matt Pietrek (2002), "Inside Windows : An InDepth Look into the Win32 Portable Executable File

Nazario, Jose, et. al., (2004), Defense and Detection Srategies Againts Internet Worms, Artech House inc., Norwood MA.

Pietrek, Mat; Peering Inside the PE A tour of the PE: A Tour of the Win32 Portable Executable File format; MSDN;1994

Reza kurniawan, (2006). Analisis serangan worms komputer,tinjauan kasus: Worm lokal email-worm.win32.brontok.c,Laporan Tugas Akhir Pada Institut Teknologi Bandung.

Richki Hardi, .(Jurnal Telematika, Vol.12,No.2, Juli 2015;p.82-98)

Szor, Peter (2005), The Art of Computer Virus Research and Defense, Addison Wesley Proffesional, New Jersey.