APLIKASI FIREWALL TERHADAP MALWARE PADA MEDIA DINAMIS

Ir. Sigit Wasista, M.Kom, Isbat Uzzin N., S,Kom, Moch. Muchlis Irvani
Jurusan Teknologi Informasi, Politeknik Elekronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember Surabaya
Kampus ITS, Keputih Sukolilo, Surabaya 60111
Telp.(+62)-31-5947280 Fax.(+62)-31-5946114
wasista@eepis-its.edu, isbat@eepis-its.edu, irvan.expert@gmail.com

Abstrak

Flashdisk merupakan salah satu dari beragam media penyimpanan yang bersifat dinamis. Keberadaannya dinilai menguntungkan sebagai pengganti era disket yang rentan / rawan cacat. Selain kapasitas yang besar, flashdisk mampu digabungkan dengan peranti lain seperti bluetooth, card reader, mp3 player dan lebih mengutamakan perpindahan data dari satu komputer ke komputer lainnya. Kesempatan kecil seperti inilah yang kerap dimanfaatkan oleh virus untuk menyebarkan "diri"-nya. Malware, definisi yang tak asing lagi yang diberikan pada para script / program asing yang bertugas merusak data dan sistem komputer, yang didalamnya termasuk juga virus, worm, dan trojan. Era baru penyebaran virus tak lagi melalui jalur internet, virus terbaru telah dapat tersebar melalui media-media penyimpanan yang sulit terdeteksi oleh antivirus. Menyadari aktivitas penyebaran virus melalui cara tersebut, saya berusaha menciptakan aplikasi sejenis antivirus yang mampu memfilter apapun yang masuk ke dalam flashdisk, jika salah satu file / data teridentifikasi sebagai virus maka akan segera diblok / dihapus. Teknik pendeteksian virus ini menggunakan CRC32 dan metode heuristic analysis untuk mendeteksi varian virus baru. Dari hasil percobaan yang telah dilakukan, teknik di atas bagus diterapkan karena mempunyai kecepatan dan level akurasi yang cukup tinggi. Babak baru sistem pertahanan terhadap virus telah dimulai.

Kata Kunci : ***Flashdisk, Malware, CRC32, Heuristic analysis***

1. Pendahuluan

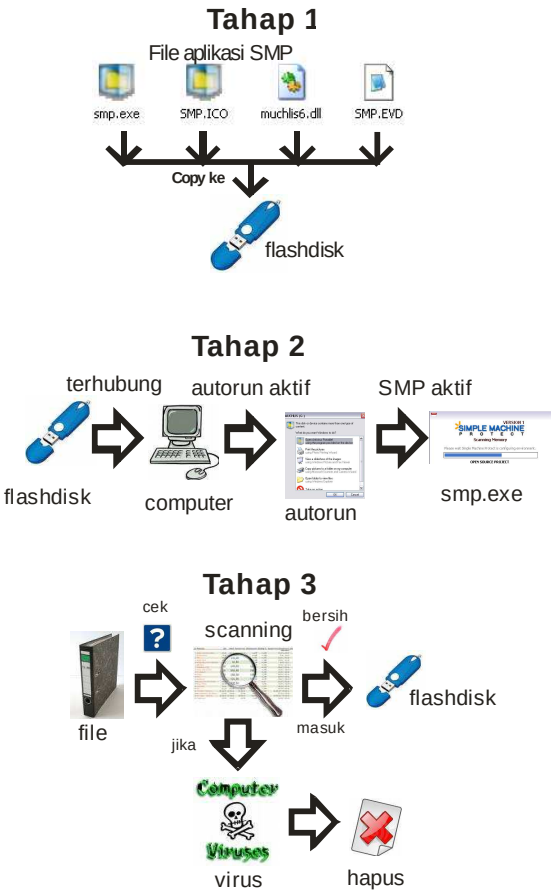
Flashdisk, disebut juga USB Flash Drive (UFD) merupakan salah satu jenis media penyimpanan data dalam kapasitas tertentu yang terbatas dan bersifat portable / dinamis. Sebagian besar masyarakat memanfaatkannya dalam bertransaksi data dari satu computer ke computer lain seperti mengambil, mengirim, menyimpan data. Tak banyak orang mengerti bahwa di dalam flashdisk tersebut memiliki kemungkinan besar terdapat suatu file yang tidak diharapkan disana. Awalnya mereka tidak menyadari bahaya besar yang akan terjadi, namun saat file asing ini beraksi, hanya dalam hitungan detik, system computer akan mengalami kerusakan yang fatal dan user akan menyalahkan orang lain atau computer tersebut tanpa menyadari bahwa ia sendiri yang membawa "bom waktu" ini.

Malware merupakan program yang paling ditakuti oleh sebagian besar masyarakat pengguna computer karena kebiasaan buruknya yang mampu merusak sistem komputer termasuk data di dalamnya. Malware dibagi menjadi beberapa jenis menurut karakteristiknya yaitu virus, worm, dan trojan. Virus merupakan program asing yang dalam tujuannya merusak sistem komputer, ia membutuhkan induk semang alias parasit pada suatu jenis file. Sedangkan worm tidak membutuhkan induk semang alias dapat berdiri sendiri. Trojan dapat mengambil informasi pribadi yang penting dari seseorang. Dari kesemua jenis tersebut, virus dan worm yang menjadi sorotan utama dalam topik ini.

Perkembangan virus lokal lebih pesat dibandingkan virus import. Para pengembang virus seakan bosan dengan hanya mengirim / menyebarkan virus melalui jaringan internet dan email. Belakangan ini penyebaran lebih ke level yang lebih rendah / spesifik dan hampir semua orang memakainya. Media seperti bluetooth, flashdisk, wireless, telah menjadi sasaran empuk bagi virus untuk berusaha masuk ke seluruh aspek komputer. Antivirus yang ada kurang fleksibel dan up-to-date dengan kemajuan virus lokal, sehingga kurang efektif dalam membangun sistem keamanan dalam komputer terutama data di dalamnya. Kami berupaya membuat aplikasi firewall yang dapat memblokir / memfilter akses masuk virus ke dalam flashdisk dengan tujuan mencegah penyebaran virus. Dengan algoritma yang telah umum dipakai oleh sebagian kalangan developer antivirus, kami memakai

algoritma CRC32 dalam mengenali virus. Dan metode analisa heuristik untuk mengenali perilaku / kebiasaan yang dilakukan virus tanpa melihat database virus yang sudah ada. Metode heuristik ini masih jarang dipakai karena jika tidak teliti, maka akan sering terjadi kesalahan pendeteksian. Namun kami berhasil mengembangkannya dan dari hasil percobaan diketahui bahwa analisa heuristik mempunyai akurasi sebanyak 87%. Hal ini menjadi lampu merah bagi para pembuat virus untuk segera meng-upgrade ilmunya atau menyerah tanpa syarat.

2. Perumusan Permasalahan



Gambar. 1. Blok Diagram Ilustrasi Perancangan Sistem

Seperti telah dijelaskan di atas, bahwa permasalahan yang kami angkat dalam penelitian ini adalah bagaimana membangun suatu aplikasi sebagai system pertahanan yang mampu mendeteksi keberadaan virus dan mencegah aksi penyebarannya baik dalam sistem komputer dan flashdisk pada khususnya.

Untuk membuat aplikasi ini digunakan system operasi windows dan menggunakan bahasa pemrograman MS. Visual Basic 6.0. Dipilih sistem operasi windows karena windows saat ini merupakan OS yang paling banyak digunakan dan paling banyak virus menyerang OS ini. Sedangkan untuk pembuat aplikasinya dipilh VB karena kemampuannya dalam berinteraksi dengan konfigurasi sistem dan administrasi windows yang sering dinamakan win32API, yang tidak dimiliki oleh bahasa pemrograman lain seperti java.

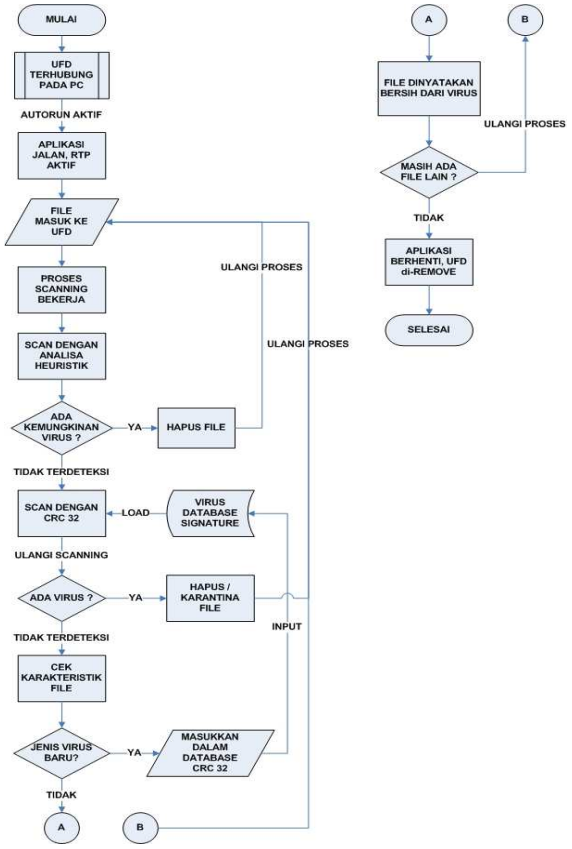
Selanjutnya kita membutuhkan tool pendukung seperti Free Hex Editor untuk mengubah isi dari suatu file yang tidak dapat dibaca dengan cara biasa dan dan dapat menganalisa kombinasi heksadesimal dari suatu string. Selain itu juga tool VB Killer seperti gasak.exe untuk mengetes sistem pertahanan dari antivirus yang kita buat apakah dengan mudah dimatikan prosesnya oleh virus atau tidak.

3. Batasan Masalah

Aplikasi ini diujikan pada PC yang terdapat virus lokal terbaru di dalamnya. PC bersifat offline dan menggunakan OS Windows XP. Asumsinya autoplay pada komputer adalah enable / aktif.

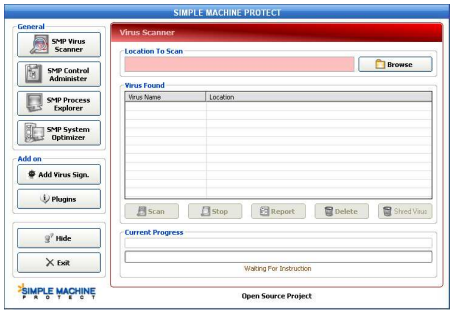
Virus yang diujikan adalah virus untuk windows dan terbatas pada sampel virus yang digunakan saja.

4. Hasil Percobaan Dan Pembahasan



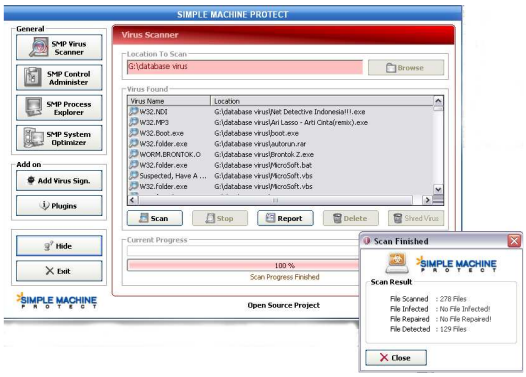
Gambar. 2. Flowchart Sistem Utama

Dalam percobaan ini dilakukan ujicoba beberapa kali. Yang pertama adalah ujicoba melakukan manual scanning dengan algoritma CRC32.

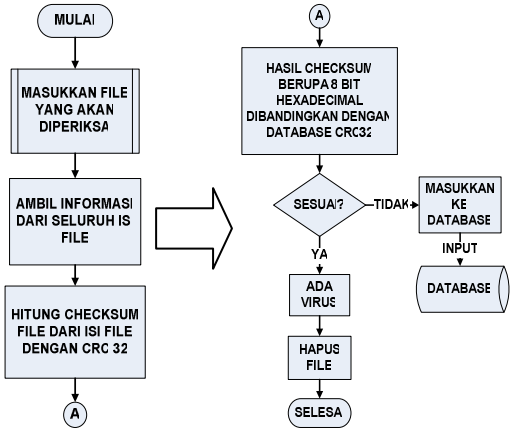


Gambar. 3. Tampilan awal aplikasi

Gambar 1 diatas merupakan tampilan aplikasi awal, beberapa sampel virus dijalankan dan lakukan proses scanning pada area tertentu.



Gambar. 4. Tampilan program hasil deteksi



Gambar. 5. Flowchart Scanning CRC32

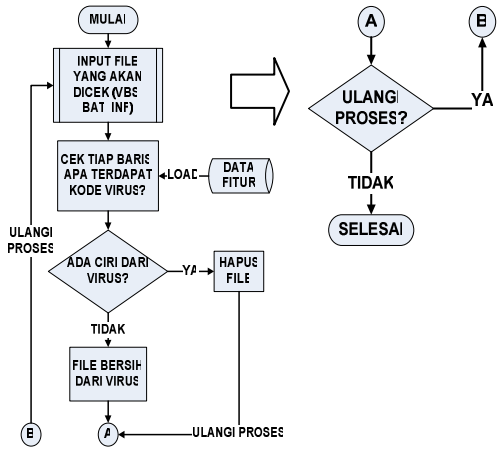
Pada gambar 2 tersebut merupakan tampilan program setelah proses pencarian / deteksi selesai dilakukan, lalu muncul report bahwa telah terdeteksi sebanyak 129 files dengan berbagai jenis virus.

Daftar hasil manual scanning dengan CRC32 :

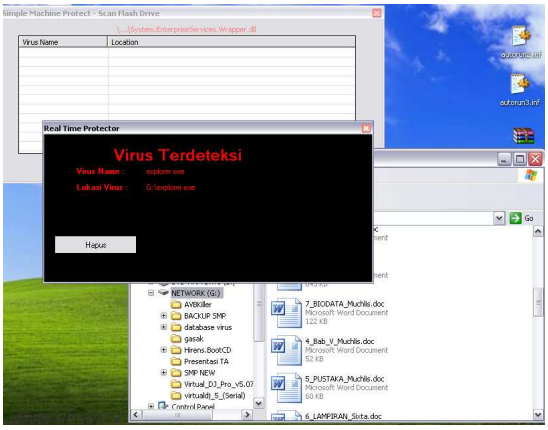
NO	NAMA VIRUS	STATUS
1	W32.NDI	Terdeteksi
2	W32.MP3	Terdeteksi
3	W32.Boot.exe	Terdeteksi
4	explorer.exe	Terdeteksi
5	W32.Brontok-Z	Terdeteksi
6	W32.found	Terdeteksi
7	W32.Khatarnak	Terdeteksi
8	W32.Lemorai	Terdeteksi
9	Brontok.C	Terdeteksi
10	RontokBro	Terdeteksi
11	Thumbs.com	Terdeteksi
12	rundll.exe	Terdeteksi
13	GavGent.B	Terdeteksi
14	Redlof.B.htt	Terdeteksi
15	Shuriken3	Terdeteksi
16	W32.JPG	Terdeteksi
17	Blackster.scr	Unknown
18	Virus Hampa	Terdeteksi
19	Sality.Q	Terdeteksi
20	Brontok.A	Terdeteksi

Tabel.1. Hasil ujicoba scanning dengan CRC32

Yang kedua adalah mendeteksi virus dengan analisa heuristik dan Real-Time Protector (RTP). Sampel virus yang diujikan adalah virus dan worm yang pada umumnya menyerang flashdisk.



Gambar. 6. Flowchart Heuristic Scanning



Gambar. 7. Tampilan hasil deteksi dengan mode heuristic dan RTP

Kemampuan deteksi mode heuristic memang terbatas pada jenis virus tertentu saja yaitu .vbs, .bat, dan .inf. Hal ini disebabkan pada umumnya jenis file inilah yang kerap menyerang flashdisk, dan diciptakannya analisa heuristik dan mode RTP untuk melindungi flashdisk dari virus.

Daftar hasil scanning dengan analisa heuristic :

NO	NAMA VIRUS	STATUS	PARAMETER
1	Autorun.inf (.vbs)	Terdeteksi	wscript
2	Autorun.inf (gondronk.vbs)	Terdeteksi	wscript
3	Autorun.inf (thumbs.com)	Terdeteksi	Heuristic mode
4	Autorun.inf (explorer.exe)	Terdeteksi	Heuristic mode
5	Autorun.inf (boot.exe)	Terdeteksi	Heuristic mode
6	Autorun.inf (myimages.exe)	Terdeteksi	Heuristic mode
7	Autorun.inf (rundll32.exe)	Terdeteksi	Heuristic mode
8	Autorun.inf (newfolder.exe)	Terdeteksi	Heuristic mode
9	Autorun.inf (newfolder.scr)	Terdeteksi	Heuristic mode
10	Autorun.inf (arilasso.exe)	Terdeteksi	Heuristic mode
11	.vbs	-	enkripsi
12	Gondronk.vbs	Terdeteksi	Heuristic mode
13	Microsoft.bat	Terdeteksi	hidden
14	Ms32.dll.vbs	Terdeteksi	Wscript.shell
15	Redlof.htt	-	unknown

Tabel.2. Hasil ujicoba scanning dengan mode Heuristic

5. Analisa

Pada percobaan pertama dapat kita lihat, dari 20 sampel virus yang diujikan hanya satu jenis virus yang tidak terdeteksi. Hal ini dikarenakan virus blackster.scr belum terdapat CRC32 checksumnya pada database sehingga tidak dikenali. Kelemahan yang paling mendasar dari scanning dengan CRC32 ini adalah terlalu mengandalkan pada virus database signature, sehingga bila terdapat varian virus baru maka belum bisa terdeteksi jika hanya memakai 1 proses scanning.

Kelemahan di atas dapat berkurang dengan adanya proses scanning yang tanpa tergantung pada database virus. Metode ini dinamakan analisa heuristik atau analisa perilaku yang dimiliki oleh virus pada umumnya. Mode heuristik ini merupakan AI(kecerdasan buatan) yang dimiliki aplikasi ini. Metode ini mengelompokkan ciri-ciri khusus yang dibawa oleh satu jenis virus tertentu misal menggunakan ”wscript.exe” pada virus autorun.inf dan sejenisnya. Namun metode ini juga mempunyai kekurangan, yaitu adanya false-alarm atau kesalahan pendeteksian pada file yang seharusnya bukan termasuk kategori virus, akan dianggap virus. Maka dari itu, kami membuat mode heuristik ini sementara hanya sesuai untuk melakukan scanning pada flashdisk saja.

Dua metode scanning dalam aplikasi ini saling melengkapi kekurangan satu sama lain sehingga mampu meningkatkan keakuratan dan efisiensi waktu dalam proses mendeteksi virus.

6. Kesimpulan

Dari hasil percobaan yang telah dilakukan dapat diambil beberapa kesimpulan, yaitu:

(1) Malware merupakan binary yang sangat berbahaya.
(2) Tingkat akurasi algoritma CRC32 adalah 95%, sedangkan analisa Heuristic adalah 87%.
(3) Aplikasi ini dapat digunakan untuk melindungi flashdisk dari penyebaran virus.
(4) Aplikasi ini mengutamakan perlindungan untuk flashdisk, meskipun dapat digunakan seperti halnya antivirus pada computer.
(5) Pada umumnya 95% virus lokal di Indonesia mempunyai karakteristik yang sama, sehingga teknik ini masih layak digunakan.

Daftar Pustaka

(1) Peter Szor. The Art of Computer : Virus Research and Defense. Symantec Press. 2005.

(2) David Harley and Andrew Lee. Heuristic Analysis : Detecting Unknown Viruses. NOD32 antivirus system. 2007. http://www.eset.com

(3) Anggiawan web forum http://putih.web.id

(4) Malware Forum http://virus.ognizer.net

(5) Analisa virus lokal http://www.vaksin.com

(6) Download sample virus lokal http://virus.ognizer.net/files/main.php

(7) Planet Source Code http://www.planet-source-code.com

(8) Jasakom virus analysis http://www.jasakom.com

(9) Yogyafree Forum http://yogyafree.net/forum

(10) VB-Bego Forum http://vb-bego.net