ANALISA KINERJA SISTEM REALTIME PROTECTOR PADA ANTIVIRUS KOMPUTER VICI

Yuni Selvita Suci [1)], Aryanti [2)], Asriyadi [3)]

Teknik Elektro, Program Studi Teknik Telekomunikasi, Politeknik Negeri Sriwijaya
Jl. Srijaya Negara, Bukit Besar, Bukit Lama, Ilir Barat, Ilir Bar. I, Kota Palembang, Sumatera Selatan 30139
Email : uciaisaka@gmail.com

Abstrak. *Pada dasarnya antivirus digunakan untuk membersihkan dan melindungi sistem komputer dari infeksi virus komputer. Namun saat ini beberapa jenis virus telah berevolusi sehingga dapat lolos dari pendeteksian antivirus, oleh karena antivirus yang digunakan belum bisa menyimpan signature dari virus tersebut. Pada penelitian ini dikembangkan sebuah aplikasi antivirus yang diberi nama Vici Antivirus yang dapat mendeteksi virus menggunakan signature dan dilengkapi dengan metode pendeteksian heuristic ganda dan sistem realtime protector. Hal yang perlu diperhatikan dalam penelitian ini untuk mengetahui bagaimana kinerja Sistem Realtime protector dalam mengoptimalkan proses scanning virus yaitu, menjalankan software antivirus guna memindai file program yang akan dijalankan dan akan menganalisis tingkat bahaya-nya. Jika terdeteksi sebagai sesuatu yang bisa membahayakan sistem, maka program antivirus akan membatalkan eksekusi dan menginformasikan adanya bahaya ke pengguna.*

Kata kunci : *virus, antivirus vici, sistem realtime protector, visual basic.*

1. Pendahuluan

Pengguna komputer tentunya pernah mengalami masalah yang di-akibatkan oleh virus baik itu secara langsung maupun tidak langsung. Hal tersebut merupakan masalah yang cukup berat karena harus membersihkan sistem komputernya dari virus secara manual. Pengguna komputer tentunya pernah mengalami masalah yang di-akibatkan oleh virus baik itu secara langsung maupun tidak langsung. Hal tersebut merupakan masalah yang cukup berat karena harus membersihkan sistem komputernya dari virus secara manual.

Virus komputer umumnya dapat merusak perangkat lunak komputer dan tidak dapat secara langsung merusak perangkat keras komputer tetapi dapat mengakibatkan kerusakan dengan cara memuat program yang memaksa *over process* ke perangkat tertentu. Efek negatif virus komputer adalah memperbanyak dirinya sendiri, yang membuat sumber daya pada komputer (seperti penggunaan memori) menjadi berkurang secara signifikan. Hampir 95% virus komputer berbasis sistem operasi Windows. Virus yang ganas akan merusak perangkat keras.[1]

Adapun tujuan yang ingin dicapai analisa kinerja *Realtie Protector* sebagai pengelompokan virus yang dirancang menggunakan software *Visual Basic* 6.0. Sistem realtime Protector Sebagai Pattern Virus, untuk mendapatkan data dan informasi yang dibutuhkan untuk laporan ini, analisa data dilakukan dengan cara mengolah data yang telah didapatkan pada tahap pengumpulan data.

2. Pembahasan

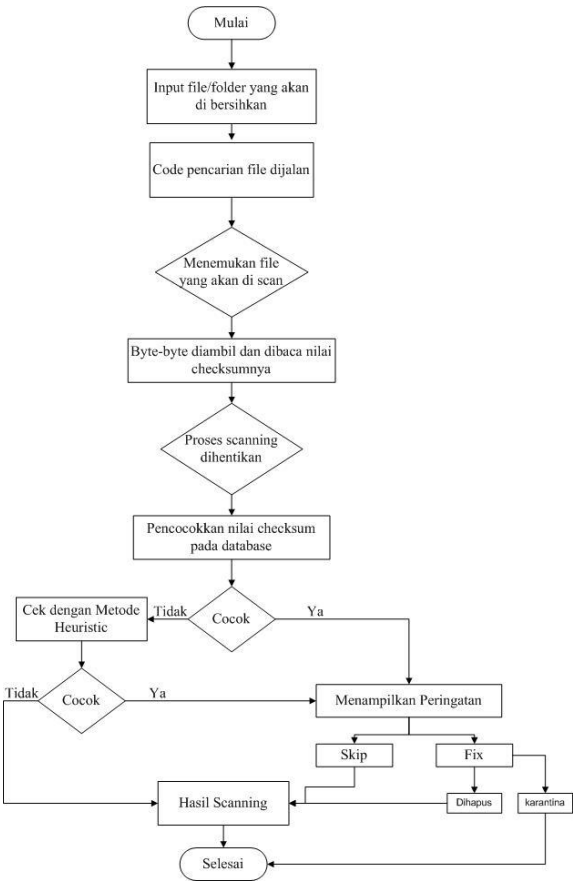
2.1 Tahap Penelitian

1. Tahapan pertama dimulai dengan mencari sampel virus ataupun worm, sampel bisa diperoleh dari file yang dicurigai sebagai sebuah virus ataupun worm berdasarkan prilakunya, dan sampel bisa juga diperoleh dari beberapa website tertentu.
2. Dari sampel virus yang diperoleh dengan metode heuristic terintegrasi langsung dalam antivirus itu sendiri.
3. Nilai dari sampel virus yang diperoleh, dimasukan langsung kedalam database antivirus dan diberi nama jenis virus atau worm nya.

4. Setelah database antivirus terisi dengan nilai-nilai dan nama virus atau worm, antivirus bisa memulai proses pencarian file virus atau worm yang terdapat dalam sistem operasi komputer sesuai dengan virus atau worm yang terdapat pada database antivirus
5. Antivirus melakukan *scanning* pada semua file yang terdapat pada sistem operasi komputer, dan menghitung nilainya.
6. Kemudian nilai yang diperoleh dari setiap file dibandingkan dengan nilai yang terdapat dalam database antivirus. Jika terdapat kesamaan maka file tersebut merupakan virus atau worm yang akan ditampilkan pada sebuah jendela list virus yang ditemui pada antivirus.
7. Berdasarkan list virus atau worm yang diperoleh, lalu akan dilakukan pengambilan keputusan untuk mengabaikan file tersebut atau me-repair file. Pada saat me-repair file maka akan menampilkan keputusan menghapus file atau dikarantina.

2.2 Perancangan *Flowchart* Antivirus *Vici*

Berikut ini tampilan *flowchart* cara kerja antivirus vici



Gambar 1. Flowchart antivirus vici

Perancangan *Flowchart* antivirus ini ialah gambaran umum dimana antivirus membaca sebuah file dan menentukan apakah file tersebut adalah sebuah virus atau bukan dengan *checksum error* pada database. Selanjutnya pada proses checksum error akan menampilkan peringatan virus itu di skip atau di fix, jika memilih skip maka virus tersebut akan langsung ke hasil scanning tanpa harus dihapus. Dan jika memilih fix maka file virus tersebut akan dihapus, proses selajutnya ke hasil scanning dan selesai. Apabila virus tersebut tidak dikenali pada database maka akan dilakukan scan dengan metode heuristic ganda, jika file tersebut cocok sebagai virus maka akan menampilkan peringatan dan jika sebaliknya maka proses selesai. *Flowchart* antivirus yang digunakan pada penelitian ini ditunjukkan dalam gambar 1.

2.3 Virus

Secara umum virus komputer merupakan sebuah *software* berbahaya (*malware*) yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menginfeksi/ menyisipkan salinan dirinya ke dalam program maupun menyebarkan program lain yang dapat dieksekusi. Beberapa kemampuan dasar virus [2], diantaranya adalah:

a. Kemampuan memperbanyak diri, yaitu kemampuan dasar sebuah virus untuk menduplikasikan dirinya pada sebuah file maupun pada sistem komputer.
b. Kemampuan menyembunyikan diri, yaitu kemampuan sebuah virus untuk menyembunyikan dirinya ketika sedang aktif (sedang menginfeksi) sehingga user tidak akan mengetahui keberadaan virus tersebut.
c. Kemampuan untuk memanipulasi, yaitu kemampuan sebuah virus dalam melakukan tindakan pada sistem, seperti membuat tampilan yang menggangu, merusak dan menghapus file dokumen atau file sistem, serta mengacaukan kerja alat-alat I/O (keyboard, printer, dan lain-lain).
d. Kemampuan mendapatkan informasi, yaitu kemampuan dasar sebuah virus untuk mendapatkan informasi tentang struktur media penyimpanan, diantara-nya letak file sistem, letak suatu file, dan sebagainya.
e. Kemampuan untuk memeriksa kebe-radaan dirinya, yaitu kemampuan dasar virus untuk mencari ID (tanda pengenal) dirinya pada sebuah file atau sistem. Kemampuan virus ini dapat mencegah virus menginfeksi sebuah file atau sistem yang sama secara berulang kali.

2.4. Antivirus Vici

Antivirus Vici merupakan antivirus yang didesain dengan metode *heuristic* ganda dan sistem *realtime protector* mengguakan software *visual basic 6.0*. Antivirus ini dapat mendeteksi dan menghapus virus, yang telah diuji dengan sample virus komputer worm dan trojan memperoleh presentasi keberhasilan 95%.

2.5. Visual Basic

Microsoft Visual basic (sering disingkat sebagai VB saja) merupakan sebuah bahasa pemograman yang menawarkan Integrated Development Environment (IDE) visual untuk membuat pemograman perangkat lunak berbasis sistem operasi Microsoft Windows dengan menggunakan model pemograman (COM). [3]

2.6. Sistem Realtime Protector

Real-time Protection adalah suatu metode yang amat penting dalam software antivirus, dalam usaha melindungi sistem komputer. Ini bisa dianggap sebagai *standar* pada program antivirus yang baik. Banyak istilah (sinonim) yang digunakan untuk fitur *real-time protection* ini. Misalnya : *Resident Shield, On-access Scanning, Background Guard, System Shield, Auto Protect* dll. Semuanya mengacu pada cara otomatis dalam melindungi komputer dari serangan malware.[4]

Pengujian sistem *realtime protector* dilakukan dengan membuka sebuah *file/folder* yang berisi virus. Jika *realtime protector* mendeteksi adanya keberadaan sebuah virus, maka *realtime protector* telah berjalan dengan baik.

Gambar 2. Hasil pengujian *Sistem Realtime Protector*.

Hasil dari pengujian sistem *realtime protector* antivirus ditunjukkan pada gambar 2. Pada gambar 2 menunjukkan sistem *realtime protector* mendeteksi sebuah file sebagai virus. Pada hasil pengujian ini, sebuah file terdeteksi sebagai virus dengan virus name "ADA.GR" dan "Atrax" merupakan virus worm. Pada Sistem realtime protector ini telah terintegrasi menggunakan metode *heuristic* ganda dan metode *checksum error*, maka akurasi pendeteksiannya sama dengan saat antivirus melakukan proses scanning.

3. Simpulan

Setelah dilakukan pengujian dan analisis kinerja *realtime protector* terhadap antivirus *vici* yang dikembangkan, maka dapat ditarik kesimpulan sebagai berikut:

1. Sistem realtime protector sangat efektif dalam melindungi sistem komputer dari serangan virus, karena mampu mendeteksi adanya keberadaan virus meskipun antivirus tidak sedang melakukan proses scanning. Sistem realtime protector telah diuji sebanyak 13 kali dengan sampel malware (virus, worms dan trojan) dan didapat rasio 95% dalam peng-ujian tersebut.
2. Berisi berbagai simpulan yang di ambil berdasarkan penelitian yang telah dilakukan. Merupakan pernyataan singkat tentang hasil yang disarikan dari pembahasan. Simpulan dapat berbentuk paragraf namun sebaiknya berbentuk point-point dengan menggunakan *numbering*.

Ucapan Terima Kasih

Saya berterima kasih kepada kedua orag tua saya yang telah membatu saya. Semoga penelitian ini sesuai apa yang akan diharapkan dan dapat bisa dikembangan kembali.

Daftar Pustaka

[1]. Dr. Solomon's Virus Encyclopedia, 1995, ISBN:1-897661-00-2, Abstract at http://vx.netlux.org/lib/aas10.html (diakses tgl 14 Novmber 2017)
[2]. http://id.wikipedia.org/wiki/Visual_Basic, diakses tgl 21 November 2017
[3]. Salim, Hartojo. 1990. *Virus Kom-puter*. Andi Offset: Yogyakarta.
[4]. http://kangtokkomputer.weebly.com/realtime-protection.html, di akses tgl 23 November 2017