JUSI Vol. 1, No. 1
Februari 2011

ISSN 2087-8737

Implementasi Virus Fr1zz sebagai Ancaman Terhadap Sistem Operasi dalam Keamanan *Registry*

Saiful Fariz, Heru Cahya Rustamaji*, Yuli Fauziah

Jurusan Teknik Informatika, UPN "Veteran", Yogyakarta
Jl. Babarsari No. 2 Tambakbayan, Yogyakarta 55281
E-mail: herucr@yahoo.com

ABSTRAK *Registry pada sistem operasi Windows XP merupakan penyimpanan informasi program pada sistem komputer. Virus komputer merupakan suatu malware yang berkemampuan berkembang biak dan memanfaatkan program lain untuk menyebarkan diri. Virus bernama fr1zz dikembangkan yang dirancang menyerang keamanan registry sehingga beberapa fungsi Windows XP dimatikan. Makalah ini juga membahas proses analisis terhadap virus fr1zz baik berupa analisis statis dan analisis dinamis serta cara menanggulangi virus fr1zz secara manual.*

***Kata kunci**: virus komputer, virus fr1zz, registry.*

1 Pendahuluan

Registry merupakan suatu basis data untuk menyimpan dan mengatur sistem di sistem operasi Microsoft Windows®. Registry merupakan otak dari sistem operasi MS Windows yang dijalankan, registry akan selalu di-*backup* dalam hitungan waktu tertentu, registry juga akan di-*backup* pada saat dilakukan *shutdown*. Modifikasi registry dapat dilakukan untuk perbaikan sistem, pengaturan untuk meningkatkan kinerja Windows, dan memanggil beberapa file pada saat startup.

Registry juga mengandung informasi konfigurasi sebuah sistem, mulai dari konfigurasi perangkat keras, perangkat lunak, asosiasi ekstensi file dengan aplikasinya sampai preferensi pengguna. Keberadaan registry yang sangat vital ini, maka registry menjadi sasaran utama virus untuk melakukan beberapa pengaturan yang terkait dengan persiapan aktivitas virus, sehingga keamanan registry menjadi sasaran utama penyerangan virus komputer agar dapat mempertahankan diri, memperbanyak diri, bersembunyi maupun menginfeksi program lain tanpa sepengetahuan pengguna komputer.

Hal ini yang melatarbelakangi penelitian tentang deteksi virus ini, karena perlu adanya pengamatan bagaimana virus itu dibuat dan analisis keamanan registry yang telah terinfeksi oleh virus sehingga dapat merusak suatu keamanan registry yang menimbulkan kerugian bagi pengguna komputer.

2 Tinjauan Pustaka

2.1 Sistem Operasi

Sistem operasi adalah suatu sistem yang terdiri dari komponen-komponen kerja dan memuat metode kerja yang digunakan untuk memanfaatkan mesin, sehingga mesin dapat bekerja sesuai dengan yang diinginkan. Fungsi utama sistem operasi sebagai media interaksi manusia dengan mesin, sehingga manusia dapat memahami mesin dan sebaliknya sehingga menjadi partner yang saling mengerti untuk melakukan suatu tugas tertentu. (Pangera dan Dony, 2005)

2.2 Virus Komputer

Istilah virus komputer sudah dikenal sejak 12 tahun yang lalu. 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. (Djojo, 1999)

Beberapa kemampuan dasar yang dimiliki oleh virus, diantaranya adalah: (Shadewa, 2006)

(a) Kemampuan untuk memperbanyak diri

Kemampuan virus untuk menduplikasi diri pada file atau disk yang belum terinfeksi, sehingga semakin lama wilayah penyebarannya semakin luas.

(b) Kemampuan untuk menyembunyikan diri

Kemampuan virus untuk menyembunyikan diri dari perhatian pengguna, antara lain dengan cara-cara berikut: (1) menghadang *output* ke layar selama virus bekerja, sehingga virus tidak tampak oleh pengguna, (2) program virus ditempatkan diluar *track-track* yang dibuat DOS, (3) ukuran virus dibuat sekecil mungkin sehingga tidak menarik kecurigaan.

(c) Kemampuan untuk mengadakan manipulasi

Kemampuan virus untuk mengadakan manipulasi yang disalahgunakan untuk: (1) membuat tampilan atau pesan yang menggangu pada layar monitor, (2) mengganti volume label disket, (3) merusak struktur disk, menghapus file-file, dan (4) mengacaukan kerja alat-alat I/O, seperti keyboard dan printer.

(d) Kemampuan untuk mendapatkan informasi

Kemampuan virus untuk mendapatkan informasi tentang struktur media penyimpanan seperti letak *boot record* asli, letak tabel partisi, letak FAT32, posisi suatu file, dan sebagainya.

(e) Kemampuan untuk memeriksa keberadaan dirinya

Sebelum menyusup ke suatu file, virus memeriksa keberadaan dirinya dalam file itu dengan mencari ID (tanda pengenal) dirinya di dalam file itu. 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.

2.3 Jenis-Jenis Virus Komputer

Jenis-jenis virus adalah sebagai berikut (Djojo, 1999):

(a) Berdasarkan teknik pembuatannya

Jenis-jenis virus berdasarkan teknik pembuatannya dibagi dalam:

- Virus yang dibuat dengan kompilator, yaitu virus yang dapat dieksekusi karena merupakan virus yang telah di-*compile* sehingga dapat dieksekusi langsung
- Virus macro, yaitu virus yang terdapat pada program Microsoft Office®.
- Virus script/batch, yaitu virus batch karena dulu terdapat pada file batch yang terdapat pada DOS, sekarang hal ini telah berganti menjadi script. Virus script biasanya sering didapat dari Internet karena kelebihannya yang fleksibel dan bisa berjalan pada saat kita bermain internet,

(b) Berdasarkan infeksi yang dilakukan

Jenis-jenis virus berdasarkan infeksi yang dilakukan dibagi menjadi tujuh, yaitu: (Shadewa, 2006)

- Virus boot sector, adalah virus yang memanfaatkan gerbang hubungan antara komputer dan media penyimpan sebagai tempat untuk menularkan virus.
- Virus file, merupakan virus yang memafaatkan suatu file yang dapat diproses langsung pada editor DOS, seperti file berekstensi COM, EXE, beberapa file overlay, dan file BATCH.
- Virus sistem, merupakan virus yang memanfaatkan file-file yang dipakai untuk membuat suatu sistem komputer.
- Virus hybrid/multi partition, merupakan virus yang mempunyai dua kemampuan biasanya dapat masuk ke boot sector dan juga dapat masuk ke file.
- Virus registry Windows, yaitu virus yang menginfeksi sistem operasi Windows 95/98/NT yang memanipulasi registry Windows, sehingga setiap kali Windows dijalankan maka virus akan dieksekusi oleh registry tersebut.
- Virus program aplikasi, merupakan virus makro, menginfeksi pada data suatu program aplikasi tertentu. Virus ini baru akan beraksi apabila program aplikasi tersebut dijalankan dan membuka data yang mengandung virus.
- Virus *Polymorphic*, yaitu jenis virus makro yang cukup cerdas karena mampu mengubah struktur dirinya untuk mengelabui anti virus yang hanya menggunakan *checksum* standar.

2.4 Cara Kerja Virus

Cara kerja virus dalam memanfaatkan registry tersebut dibagi menjadi 5 cara, yaitu: (Shadewa, 2006)

(a) Virus menginfeksi melalui pemicu registry

Pada registry ini berguna untuk memicu file virus, sehingga virus otomatis akan aktif jika Windows masuk. Alamat registry tersebut adalah

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
```

(b) Virus menginfeksi melalui penyembunyian ekstensi file

Cara kerja virus ini berfungsi untuk mengelabui user karena ekstensi file tersebut disembunyikan. Alamat registry tersebut adalah

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\
```

(c) Virus menginfeksi melalui registry penyembunyian file yang beratribut *hidden*

Cara kerja virus tersebut adalah dengan menyembunyikan diri, virus tersebut menginfeksi suatu file yang atributnya adalah *hidden*. Virus tersebut berpura-pura menjadi file sistem di Windows untuk menginfeksinya. Alamat registry tersebut adalah

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advance\
```

(d) Virus menginfeksi melalui registry edit

Cara kerja virus tersebut adalah dengan mengunci *regedit* yang ada di Windows, sehingga pada saat pengguna akan masuk ke pengolah registry (*regedit*) maka regedit tersebut dimatikan oleh virus sehingga tidak dapat dibuka. Alamat registry tersebut adalah

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Polices\System\
```

(e) Virus menginfeksi melalui *system editor*

Cara kerja virus tersebut adalah dengan menginfeksi file-file tertentu yang dijalankan ketika komputer masuk ke sistem Windows pertama kali. Nama file-file yang diserang tersebut adalah Config.sys, Autoexec.bat, Win.ini, dan System.ini

2.5 Exploit Windows

Eksploitasi yang dapat dilakukan oleh virus dan pemrograman malware supaya dapat bekerja terdiri atas: (Wardana, 2008)

(a) Eksploitasi Pengecekan

Eksploitasi ini digunakan untuk melakukan pengecekan keberadaan dan menjalankan virus secara otomatis tanpa campur tangan baik programmer maupun korban.

1. Eksploitasi Registry

   Banyak informasi yang disimpan oleh registry, untuk itu tempat penyimpanan dikelompokkan ke dalam beberapa tempat. Registry menggunakan 5 buah root utama pada Windows XP yaitu:

- HKEY_CLASSES_ROOT Berisi data semua asosiasi tipe asosiasi file, informasi OLE *(Object Linking and Embedding)* dan *shortcut* data.
- HKEY_CURRENT_USER Berisi informasi setting user yang sedang *log on*.
- HKEY_LOCAL_MACHINE Berisi informasi tipe hardware, software dan sistem konfigurasi.
- HKEY_USER Berisi semua informasi setting user.
- HKEY_CURRENT_CONFIG Berisi konfigurasi hardware.

2. Eksploitasi Folder StartUp

Ada lokasi folder di Windows yang jika ditempatkan program di dalamnya maka program tersebut akan dijalankan secara otomatis saat Windows di hidupkan pertama kali.

Jika program virus atau file link virus diletakkan di lokasi tersebut maka virus akan berjalan secara otomatis saat Windows XP dihidupkan pertama kali. Data alamat folder startup sebenarnya terdapat di registry di lokasi

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell
Folders
```

pada nilai StartUp terdapat data nilai alamat folder startup tersebut sehingga alamat default bisa dirubah menuju lokasi lain yang diinginkan.

3. Eksploitasi File Autoexec.bat

File autoexec.bat adalah file yang terletak di *root* folder seperti C:\ dan isi file autoexec.bat akan dijalankan secara otomatis setiap kali sistem operasi dijalankan. Di dalamnya bisa dimasukkan entry ke dalam file ini untuk program–program yang hendak dijalankan secara otomatis.

4. Eksploitasi Nama Program

Dengan sedikit manipulasi di registry ketika korban mengetikkan "msconfig" yang dijalankan program lain, bisa juga virus. Letak alamat manipulasi registrynya di

```
HKLM\Software\Microsoft\Windows\Currentversion\AppPath
```

pada alamat registry tersebut terdapat kunci-kunci nama file program. Pada kunci tersebut terdapat nilai default yang berisi data alamat program msconfig. Jika mengganti alamat tersebut dengan alamat tempat virus maka akibatnya ketika memanggil "msconfig" maka yang dijalankan adalah program virus.

5. Eksploitasi Handle File

Ketika suatu file dibuka, maka Windows akan membaca ekstensinya terlebih dahulu. Windows akan membuka daftar kunci di HKCR. Berdasarkan nilai default, diperoleh data untuk menangani ekstensi tersebut. Alamat registry yang bisa dimanipulasi di `HKCR\exefile\shell\open\command` data nilai defaultnya diubah dari "%1

%*" menjadi "`file.exe %1 %*`" yang merupakan alamat program virus saat program berekstensi exe dijalankan.

6. Eksploitasi Debugger Program

Ada alamat registry yang menyebabkan saat program dipanggil maka yang berjalan adalah program lain, yaitu dengan memanfaatkan debugger program, alamatnya ada di:

```
HKLM\software\microsoft\WindowsNT\ImageFileExecution\(namaprogram)
```

7. Eksploitasi Inject File Program

Virus masuk dan bergabung ke dalam tubuh file program yang diinfeksi sehingga ketika menjalankan program tersebut virus langsung bekerja. Untuk memisahkan dilakukan dengan memisahkan *header* file program asli dengan *header* program virus.

8. Eksploitasi Shortcut Program

Untuk menjalankan program yang telah terinstall di komputer maka bisa menggunakan fasilitas *shortcut* dengan cara pilih tombol Start, pilih program selanjutnya pilih program yang diinginkan. Sebenarnya yang diklik adalah file shortcut pada suatu folder misalnya di C:\Document and Setting\All Users\Start Menu\Programs\ atau di C:\Document and Setting\(nama account)\Start Menu\Programs\. Folder-folder tersebut terdiri atas file-file shortcut yang jika dijalankan maka file *shortcut* tersebut akan memanggil suatu program di folder Program Files.

(b) Eksploitasi Manipulasi

Selain menggunakan eksploitasi untuk menyebarkan diri virus juga menggunakan eksploitasi manipulasi untuk memanipulasi pada kinerja sistem operasi dan digunakan untuk melakukan *blocking* terhadap beberapa kinerja sistem operasi sehingga virus dapat bekerja secara aman dan korban tidak menyadari sistem operasi mereka telah terinfeksi.

1. Eksploitasi Mematikan Program Berbahaya

Program berbahaya di sini merupakan program-program yang dianggap berbahaya bagi kelangsungan virus tersebut. Program yang sering dimatikan oleh program virus adalah:

- *Task Manager* Program bawaan ini cukup berbahaya karena memperhatikan program-program yang sedang bekerja di memori.
- *Registry Editor* (regedit.exe) Program ini digunakan untuk akses ke basis data registry. Kebanyakan virus lokal mengubah nilai-nilai registry untuk menjaga eksistensinya, oleh sebab itu virus harus menjaga jangan sampai program ini dapat digunakan oleh korban.
- *System Configurasi Utility* (Msconfig.exe) Program msconfig berguna untuk menampilkan informasi program yang bekerja saat Windows dihidupkan pertama kali baik melalui *run* registry maupun folder Startup.

- Program *Tasklist.exe* dan *Taskkill.exe* Sebenarnya program-program ini dapat digunakan untuk menggantikan *task manager* dalam mematikan program yang sedang berjalan bahkan memiliki kelebihan tersendiri yaitu dapat mematikan banyak program sekaligus dengan hanya menjalankan satu file bat.
- Fasilitas *Search* Windows.
- Menu *Run* untuk mempersulit dalam mengakses regedit dan msconfig.

2. Eksploitasi Penyamaran Virus Script

Virus dapat berupa file script vbs, bat, js, cmd dan file program *executable* berupa file berekstensi exe, scr, com, pif. File ini di komputer sudah diatur gambar ikon dan keterangannya tetapi oleh virus ikon dan keterangannya dapat diubah melalui registry.

3. Eksploitasi Blockade Situs-Situs Berbahaya

Di sini virus melakukan pemblokiran website-website tempat mendownload antivirus dan forum-forum diskusi penanganan virus. Eksploitasi yang dilakukan dengan mengubah file host di alamat "C:\windows\system32\drivers\etc\". File aseli berisi: 127.0.0.1 localhost ditambah menjadi 127.0.0.1 localhost 127.0.0.1 smadav.net, sehingga user tidak dapat mengakses website smadav.net karena mengarah ke komputernya sendiri yang beralamat 127.0.0.1.

2.6 Analisa Virus

Pada dasarnya untuk menganalisa virus ada 2 tahapan, yaitu: (Wardana, 2008)

(a) Analisa Statis

Analisa statis yaitu virus yang akan dianalisis tidak dioperasikan, hanya menganalisa kode-kode di dalamnya dengan cara: (1) membaca info *header* program, (2) melihat *data resource* program, (3) *disassembling* kode untuk mempelajari tingkah lakunya, dan (4) *dependency scanning* untuk mengetahui file *library* atau program yang terkait dengan virus.

(b) Analisa Dinamis

Analisa dinamis yaitu virus dioperasikan untuk menyerang sistem operasi dan dipelajari sifat dan cara kerja virus tersebut melalui: (1) analisa proses virus di memory, (2) analisa keamanan registry, (3) analisa akses file sistem untuk mengetahui persebaran birus, (4) analisa perubahan sistem Windows, baik sistem file maupun registry.

3. Pembahasan

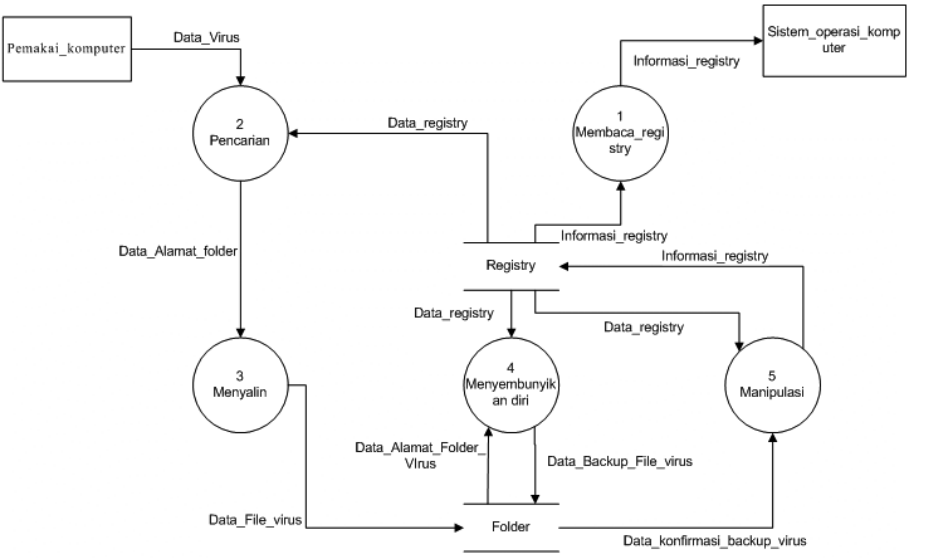
3.1. Analisis Sistem

Pada mekanisme interaksi virus dengan sistem merupakan kerja sifat dan perilaku dasar dari virus, di antaranya yaitu: pencarian, menyalin, menyembunyikan diri dan manipulasi. Keempat perilaku tersebut akan

bekerja pada sistem komputer korban yang akan diinfeksi. Output yang akan didapat dari virus *fr1zz* ini adalah menjalankan virus di *startup*, mematikan menu Run di tombol Start, mematikan fasilitas pencarian, mematikan penggunaan program registry, mematikan penggunaan *task manager*, menyembunyikan tampilan file tersembunyi di Windows Explorer dan mematikan penggunaan file *inf* yang berguna untuk mengakses registry.

3.2 Perancangan Sistem

Pemakai_komputer melakukan interaksi terhadap virus sehingga proses virus berjalan dan Sistem_operasi_komputer sebagai object yang terinfeksi dengan adanya perubahan registry yang terjadi pada proses virus. Pada Sistem_operasi_komputer menerima informasi perubahan registry yang harus dirubah.



Gambar 1. Data Flow Diagram Kerangka Kerja Virus *Fr1zz*

DFD pada Gambar 1 menggambarkan kerangka kerja virus *fr1zz* yang terdapat 4 proses yang didasari dari sifat dan perilaku komputer: menyembunyikan diri, menyalin, pencarian, dan manipulasi ditambah satu proses membaca_registry.

3.3 Implementasi Sistem

Disini akan dilakukan tahapan analisis virus *fr1zz*, akan dilakukan 2 tahapan untuk menganalisis virus *fr1zz* yaitu analisis statis dan analisis dinamis.

3.3.1 Analisis Statis

Analisis statis ini akan menggunakan program tambahan yaitu PE Explorer dengan tahapan sebagai berikut:

(a) virus *fr1zz* dijalankan menggunakan PE Explorer, terlihat virus *fr1zz* telah di-*decompress* menggunakan UPX untuk memperkecil ukuran aslinya, dari 460 KB menjadi 233 KB.

(b) mengidentifikasi kode sumber program virus *fr1zz*, terlihat ada RC data yang berisi tentang *packageinfo* bahwa program virus ditulis menggunakan bahasa Pascal (Delphi).
(c) mengidentifikasi nilai string, virus *fr1zz* ternyata ditulis menggunakan program Delphi. Besar kemungkinan virus menggandakan diri ke beberapa folder tersebut. Pada proses *disassemble* juga terlihat penggandaan nama-nama virus yang disebarkan.

3.3.2 Analisis Dinamis

Virus *fr1zz* akan dijalankan pada mesin virtual VMWare 6 yang bersistem operasi Windows XP, dan program tambahan untuk menangkap tingkah laku virus *fr1zz* menggunakan Landesk Thinstall.

Langkah-langkah analisis:

(a) Menjalankan Landesk Thinstall

Melakukan *pre-install scan* untuk menangkap data Windows XP sebelum virus dijalankan, kemudian virus *fr1zz* dijalankan dan dilakukan *scan* ulang.

(b) Menjalankan Process Explorer

Virus *fr1zz* menjalankan process MSConfig.exe yang merupakan penggandaan dirinya menggunakan *process manager*, karena *task manager* dan menu *run* telah di-*block* oleh virus *fr1zz*.

(c) Membuka Hasil capture Landesk Thinstall

Hasil tangkapan Landesk Thinstall terhadap virus *fr1zz* diperoleh informasi berikut:

Virus *fr1zz* membuat file dengan nama MsConfig.exe yang beratribut hidden pada folder AppData. Di folder personal virus *fr1zz* membuat file fr1zz.js dan di folder My Music terdapat file fr1zz.jpg. Di folder startup virus *fr1zz* menggandakan dirinya dengan nama sama dengan induk virus. Ada 3 buah rekaman perubahan registry yang dilakukan virus fr1zz yaitu HKEY_CURRENT_USER.txt, HKEY_LOCAL_MACHINE.txt, dan HKEY_USERS.txt.

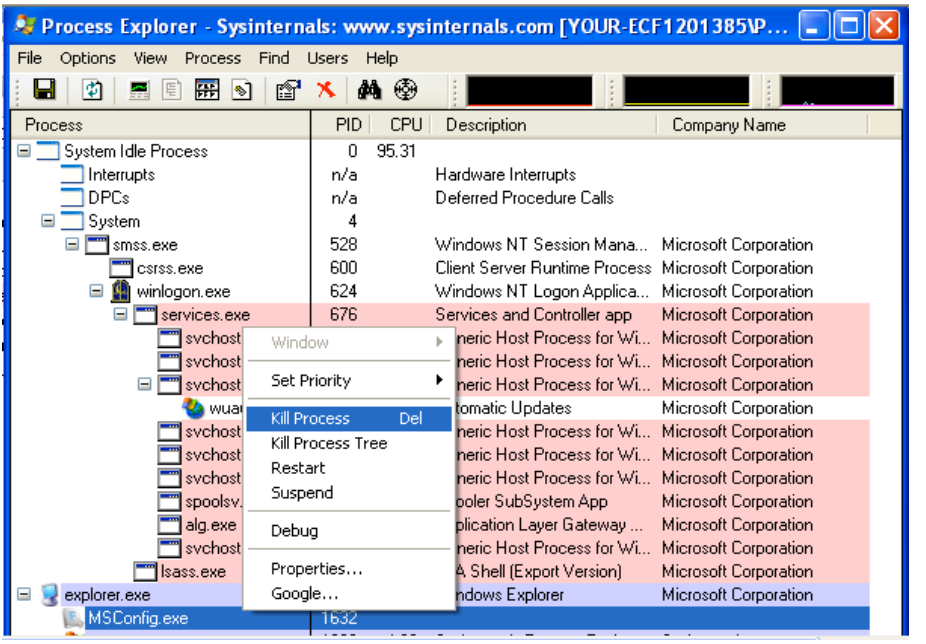
3.3.3 Penanggulangan Virus Fr1zz

Di sini akan dibahas penanggulangan virus *fr1zz* secara manual tanpa bantuan antivirus karena virus *fr1zz* tersebut masih belum terdeteksi oleh beberapa antivirus. Dari informasi analisis yang diperoleh baik analisis statis maupun analisis dinamis dapat dilakukan berbagai cara untuk mematikan virus fr1zz, yaitu:

(a) Mematikan process virus *fr1zz*

Windows XP memiliki program bawaan untuk mematikan proses yang sedang berjalan dengan menggunakan taskmanager, akan tetapi virus *fr1zz* telah mem-*block* taskmanager tersebut, untuk itu diperlukan program *Process Explorer*

(Gambar 2) untuk mematikan proses MsConfig.exe yang merupakan hasil penggandaan virus *frizz*.



Gambar 2. Mematikan proses menggunakan *Process Explorer*

(b) Menghapus penggandaan dan cadangan virus *frizz*

- di folder My Document terdapat frizz.exe.
- di folder startup terdapat frizz.exe.
- di folder ApplicationData terdapat Msconfig.exe yang beratribut hidden.
- di folder My Music terdapat frizz.jpg yang beratribut hidden.
- di folder My Document terdapat frizz.js.

(c) Memperbaiki Registry

Fungsi *run* dan *regedit* tidak dapat digunakan karena di block oleh virus maka digunakan bat file untuk membuka kembali fungsi *run* dan *regedit*.

(d) Menjalankan fungsi *run* dan *regedit* , yaitu:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\policies\system\
```

DisableTaskMgr diganti nilainya menjadi 0 agar *task manager* berjalan normal lagi.

```
HKCU\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\
```

NoFind diganti nilainya menjadi 0 agar fungsi pencarian berjalan normal lagi.

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hi
deFileExt
```

diganti nilainya menjadi 0 agar ekstensi file muncul normal lagi.

Menjalankan penggunaan file inf di

```
HKCR\ inffile\shell\Install\command
```

dengan mengganti nilainya menjadi %SystemRoot%\System32\rundll32.exe setupapi, InstallHinfSection DefaultInstall 132 %1.

4 Kesimpulan

Keamanan *registry* menjadi sasaran utama dalam mematikan beberapa fungsi Windows XP yang sedang bekerja. Terdapat empat fungsi dalam pengembangan virus yaitu pencarian, menyalin, menyembunyikan diri dan manipulasi. Analisa virus dibagi menjadi dua macam yaitu analisa statis dan analisa dinamis. Sebaiknya setiap pengguna komputer dapat mengetahui cara menganalisa virus, sehingga lebih mudah dalam penanganan dan penanggulangan dari infeksi virus dan menjadi antivirus sendiri terhadap sistem operasi yang sedang dipakainya.

Referensi

Djojo, M. (1999), "Konsep Perlindungan Komputer terhadap Virus", tersedia di http://www.arcle.net (diakses 13 Maret 2010).

Pangera, A. A. dan Dony A. (2005), *Sistem Operasi*, Yogyakarta: Andi.

Shadewa, A. (2006), *Libas Virus Lokal*, Yogyakarta: DSI Publishing.

Wardana, (2008), *Virus Kung Fu*, Jakarta: Jasakom.

Windows XP, tersedia di http://id.wikipedia.org/wiki/Windows_XP (diakses 13 November 2010).

***