METODA PERTAHAN DIRI PROGRAM VIRUS

JUFRIADIF NA'AM
Universitas Putra Indonesia YPTK Padang
Padang – Sumatera Barat – Indonesia – 2012

ABSTRACT

Virus is a computer program to duplicate or replicate by inserting copies of itself storage or document and to the network secretly. Perform the functions of the Form Load, duplicate to the system, alter modify the registry and damage the system. The results of the design of this virus can know how this virus works on the Windows operating system.
Key word :
Virus, worm, registry, malware

PENDAHULUAN

Saat ini, istilah virus komputer memang tidak asing lagi bagi kalangan pengguna komputer. Pada tahun 1988, muncul artikel-artikel di beberapa media yang dengan gencar memberitakan mengenai ancaman baru bagi para pemakai komputer yang kemudian dikenal dengan sebutan "virus komputer". Virus dengan tujuan yang bermacam-macam, pada awalnya pembuat virus membuat sebuah virus dengan tujuan untuk memberikan sistem keamanan terhadap komputer yang dimilikinya oleh orang-orang yang tidak berhak menggunakan komputer tersebut dengan tujuan merusak dan mengacaukan sistem komputer yang ditularinya.

Virus adalah sebuah program komputer yang memiliki kemampuan untuk menggandakan diri dengan cara menyisipkan programnya ke dalam sebuah file lain. Mirip seperti virus biologis, virus komputer dapat menyebar dengan cepat pada file-file dalam sebuah komputer, atau bahkan menulari file di komputer lain, baik melalui jaringan maupun lewat kegiatan tukar-menukar file.

Virus merupakan keluarga dari *malware (malicious software)* atau software yang berbahaya. Tidak hanya virus, *malware* bisa juga berupa *trojan, spyware, worm, keylogger*, dan jenis lainnya. Pada kenyataannya, cara kerja *malware* hampir sama, tetapi dengan tujuan berbeda. Dari beberapa jenis *malware* yang paling banya menghantui pengguna komputer di Indonesia adalah *worm* dan virus. *Worm* dan virus yang dibuat bertujuan untuk merusak dan mengacaukan sistem komputer. Berbeda dengan *trojan, spyware dan keylogger* yang biasanya ditujukan untuk mencuri informasi dari korban.

Sifat dasar virus komputer adalah mampu memodifikasi dan menginfeksi program lain sebagai media penyebarannya. Pada dasarnya, penggunaan istilah virus dikarenakan adanya kesamaan dalam hal sifat antara virus komputer dengan virus biologis. Dimana keduanya memiliki dua tujuan untuk bertahan hidup dan bereproduksi.

DAMPAK YANG DITIMBULKAN VIRUS

Dampak dari virus komputer sangat beragam mulai dari muncul komputer menjadi lambat, muncul pesan, gambar aneh, merusak sistem komputer, serta merusak dan menghapus file atau dokumen korbannya.

1. Memperlambat Kinerja Komputer
   Hampir semua virus yang pernah menyebar akan menyebabkan kinerja komputer manjadi lambat. Ini dikarenakan setiap virus yang masuk atau menginfeksi komputer akan berusaha menjadi host atau penguasa dari sistem yang diinfeksi. Itulah sebabnya berbagai proses pemantauan dan manipulasi wajib virus jalankan perwaktu, yang menyebabkan virus sangat membebani kinerja komputer, apalagi komputer dengan spesifikasi standar. Untuk menginfeksi komputer, virus menggunakan code berikut:

   ```
   CopyFile Left$(GetWindowsPath, 3) & "HerCoolest3.exe", NamaPath(sFilePath) & RTrim$(Left(NamaFile(sFilePath), Len(NamaFile(sFilePath)) - 4)) & ".exe", 0
   ```

   Penggunaan code di atas bisa digunakan lebih dari satu kali. Fungsi code di atas agar virus mengkopikan diri ke direktori Windows. Untuk memperbanyak file host dari virus maka kita tinggal menggunaka code yang sama namun melakukan perubahan pada file nama dari virus, misalnya file nama virus "HerCoolest3.exe" diganti menjadi "System.exe".
2. Menginfeksi File *Executable*
   Program maupun aplikasi adalah komponen yang kita gunakan dalam berinteraksi denga perangkat-perangkat lunak maupun keras pada komputer. Virus mampu menginfeksi file executable sehingga ketika kita menjalankan sebuah aplikasi yang telah terinfeksi virus, kita juga akan menjalankan virus yang bersembunyi di dalam aplikasi tersebut. Virus yang mampu melakukan hal ini jumlahnya masih sangat terkendali. Hal itu dikarenakan hanya orang-

orang tertentu yang mampu membuat virus dengan teknik khusus ini.
File hasil pekerjaan kita pada Ms. Word dan Ms. Excel sebagian besar berformat *.doc dan *.xls. Pada beberapa virus tertentu bisa menginfeksi file tersebut hanya untuk sebuah alasan konyol virus, yaitu untuk mempertahankan, mengekspansi serta memberitahukan keberadaan dirinya. Di samping itu, kita sangat dirugikan karena file penting kita tidak akan bisa dibuka dengan normal tanpa langkah pembersihan terlebih dahulu.
Ketika proses menginfeksi dan memodifikasi file yang akan dijadikan targer oleh virus, virus akan melakukan pencarian direktori file yang akan diinfeksi dengan menggunakan code berikut:

sFilePath = Right$(Command$, Len(Command$) - 1)
sFilePath = Left$(sFilePath, Len(sFilePath) - 2)

Apabila file yang akan diinfeksi telah ditemukan, virus akan memodifikasi atribut dari file tersebut dengan code berikut:

SetFileAttributes sFilePath, FILE_ATTRIBUTE_HIDDEN Or FILE_ATTRIBUTE_READONLY

Code di atas berfungsi untuk mengubah atribut dari file yang sebelumnya normal menjadi *Read Only* dan *Hidden.* Setelah memodifikasi atribut dari file yang menjadi target dari virus, virus akan mengkopikan diri ke folder lokasi file tersebut dengan code berikut:

CopyFile Left$(GetWindowsPath, 3) & "HerCoolest3.exe", NamaPath(sFilePath) & RTrim$(Left(NamaFile(sFilePath), Len(NamaFile(sFilePath)) - 4)) & " .exe", 0

Pada code di atas, file virus yang ada pada direktori Windows dengan nama "HerCoolest3.exe" akan mengkopikan diri ke folder file yang telah dimodifikasi dengan nama yang sama dengan nama file yang telah dimodifikasi dan kemudian ditambahkan spasi sehingga apabila file yang diinfeksi bernama "Antivirus.exe", file virus yang akan dikopikan akan bernama "Antivirus .exe". Karna file asli telah dirubah atributnya dan disembunyikan, pengguna komputer akan tertipu ketika ingin menjalankan file "Antivirus.exe". Sehingga pengguna komputer yang telah terinfeksi akan menjalankan kembali file dari virus.

3. Mendatangkan Virus Lain
   Mungkin dampak ini akan dirasakan oleh sebagian orang ketika terinfeksi virus tertentu, khususnya pengguna yang terkoneksi denga internet. Hal ini sangat merepotkan terutama jika kita akan melakukan pembasmian virus, yang semula lebih mudah akan menjadi sangat sulit karena virus yang menginfeksi komputer kita akan mendatangkan virus lain dengan mengunduhnya secara otomatis pada alamat-alamat web tertentu.
4. Mencegah Akses Ke Web Tertentu
   Ketika kita berhadapan dengan sebuah virus, pikiran kita akan tertuju untuk meminta bantuan pihak-pihak yang lebih ahli dalam menanganinya. Salah satunya melalui internet, dengan mengunduh produk atau mengakses web-web yang menyediakan solusi-solusi pembasmi virus. Namun, beberapa pada virus akan memblokir web-web security yang akan kita kunjungi.

Disamping itu, dalam mempertahankan diri, virus akan memperlihatkan eksistensi/keberadaannya serta mengubah/memanipulasi registry. Berikut beberapa ulah yang biasa dilakukan virus pada registry:

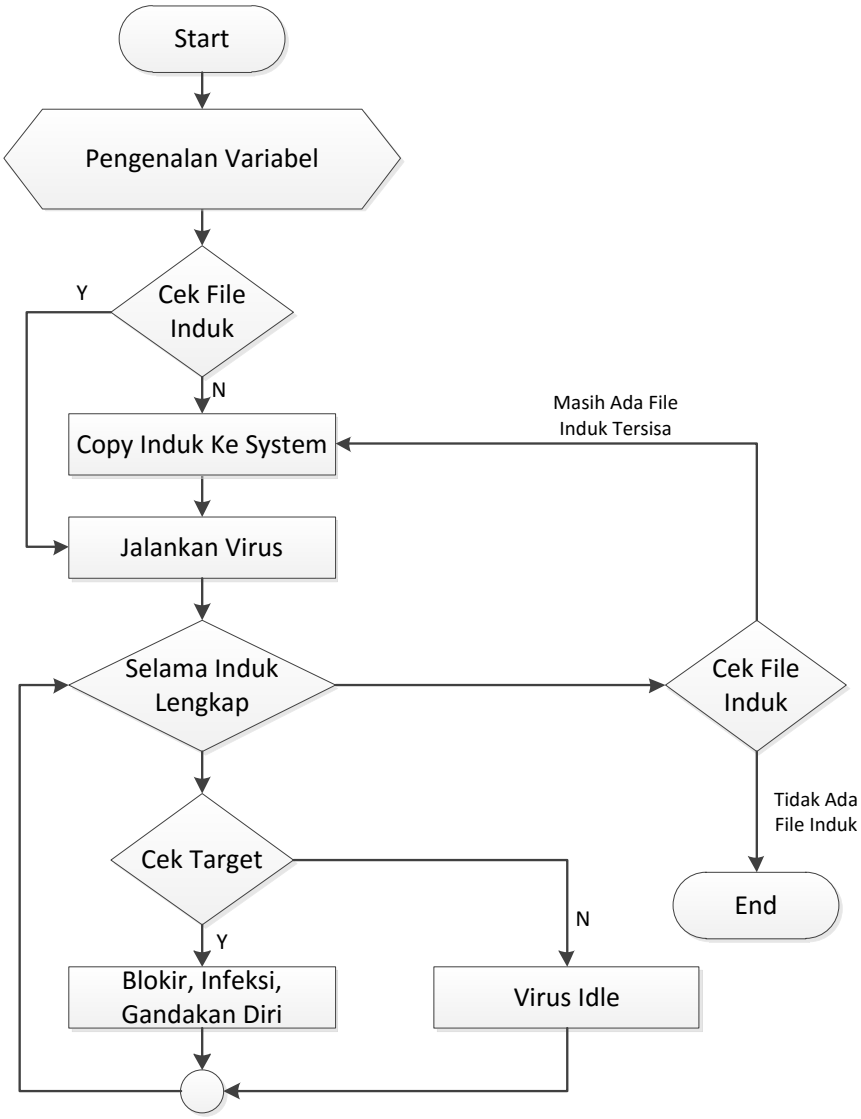
1. Mengaktifkan Virus
   Virus harus aktif saat komputer mulai dinyalakan. Untuk itu, virus harus menuliskan alamat Start-Upnya. Biasanya alamat registry yang dimanipulasi oleh virus adalah:
   HKCU\Software\Microsoft\Windows\CurrentVersion\Run
   HKLM\Software\Microsoft\Windows\CurrentVersion\Run
2. Menyembunyikan Ekstensi File
   Biasanya virus menyembunyikan ekstensi file agar dapat menipu user, sehingga user seolah-olah menjalakan file asli. Padahal, user tersebut telah menjalankan virus. Alamat registry yang dimanipulasi oleh virus adalah:
   Alamat : HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
   Key : HideFileExt
   Value : 1
3. Menyembunyikan File
   Untuk mempertahankan kelangsungan hidupnya, virus biasanya menyembunyikan diri dengan mengatur file beratribut hidden. Alamat registry yang dimanipulasi oleh virus adalah:
   Alamat : KCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
   Key : Hidden
   Value : 1
4. Memblokir Registry
   Virus biasa mengunci registry agar semua manipulasi yang dilakukan pada registry tidak diubah kembali. Alamat registry yang dimanipulasi oleh virus adalah:

Alamat : HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Key : DisableRegistryTools
Value : 1

5. Memblokir Task Manager
   Agar proses virus tidak mudah dimatikan, virus melakukan manipulasi terhadap registry untuk memblokir Task Manager. Registry yang dimanipulasi oleh virus untuk menutup Task Manager adalah:
   Alamat : HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
   Key : DisableTaskMgr
   Value : 1
6. Memblokir Command Prompt
   Kita sering menggunakan Command Prompt untuk melakukan manipulasi-manipulasi melalui jendela DOS. Karena fungsi tersebut, biasanya virus akan memblokir Command Prompt agar virus dapat mempertahankan dirinya. Registry yang dimanipulasi oleh virus untuk memblokir Command Prompt adalah:
   Alamat : HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
   Key : DisableCMD
   Value : 1
7. Memblokir System Restore
   Ketika komputer kita terkena virus, mungkin kita berpikir untuk mengembalikan komputer ke keadaan sebelumnya. Caranya adalah dengan menggunakan System Restore. Namun, virus sering melakukan pemblokiran terhadap System Restore. Registry yang dimanipulasi oleh virus untuk memblokir System Restore adalah:
   Alamat : HKLM\Software\Policies\Microsoft\WindowsNT\SystemRestore
   Key : DisableSR
   Value : 1
8. Mengubah Gambar Pada Desktop/Wallpaper
   Virus mempunyai teknik untuk memperlihatkan eksistensi/keberadaanya dengan mengubah gambar pada desktop/wallpaper. Registry yang dimanipulasi oleh virus untuk mengubah gambar di wallpaper adalah:
   Alamat : HKCU\Control Panel\Desktop
   Key : Wallpaper
   Value : Alamat gambar yang dijadikan wallpaper
9. Mengubah Tampilan Jam Menjadi Nama Virus
   Selain wallpaper, virus memperlihatkan eksistensi/keberadaannya dengan mengubah tampilan jam. Registry yang dimanipulasi oleh virus untuk mengubah tampilan jam menjadi nama virus adalah:
   HKCU\Control Panel\International\s1159-AM
   HKCU\Control Panel\International\s2359-PM
10. Mengunci Folder Options
    Registry yang dimanipulasi oleh virus untuk mengunci Folder Options adalah:
    Alamat : HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
    Key : NoFolderOptions
    Value : 1

ALUR KERJA PROGRAM VIRUS

Alur kerja program virus merupakan bagian terpenting yang menggambarkan kerja dari virus sehingga lebih mudah untuk dipahami.



Gambar 1. Flowchart Alur Kerja Virus

FUNGSI-FUNGSI YANG DIGUNAKAN

Berikut ini adalah beberapa fungsi yang terdapat dalam teknik pemrograman pertahan diri aplikasi Virus :

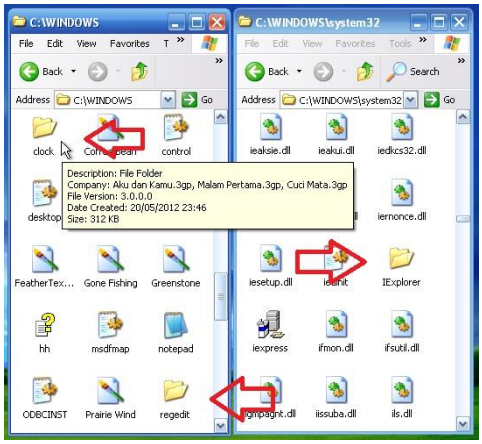
a. Fungsi ganda ke sistem
   Fungsi kode yang dimaksud adalah untuk menggandakan virus setelah berjalan di sistem yang telah diinfeksi, kemudian menggandakan diri ke sistem pada folder *Windows* dan *System32*
b. Fungsi ganda ke lokasi lain
   Merupakan kode yang mampu membuat virus bisa menggandakan diri bukan hanya pada lokasi sistem saja, tetapi juga ke partisi atau *drive* lain.
c. Fungsi *Get Files*
   Kode tersebut bertujuan untuk mendapatkan informasi dari data yang dijadikan target oleh virus. Setelah mendapatkan target, maka virus akan menyembunyikan data tersebut dan digantikan oleh virus.
d. Fungsi infeksi
   Fungsi infeksi merupakan kode yang bertujuan agar membuat virus menyerang dan memanipulasi sistem dengan merubah dan menambahkan pengaturan yang mampu menipu pengguna komputer yang awam.

1. Menggandakan Diri Ke Sistem

Proses menggandakan diri ke sistem berfungsi agar virus tetap aktif pada saat komputer mulai aktif. Biasanya hasil penggandaan ke sistem mempunyai nama yang serupa dengan nama *file system* atau mirip, namun ada juga yang sama dengan *file system* namun pada lokasi yang berbeda.

Ketika virus dijalankan, virus tersebut akan memulai aktivitasnya dengan melakukan penggandaan ke sistem komputer. Hal ini dilakukan agar virus tetap berada pada sistem meskipun sarana penyebarannya telah dilepas.

Lokasi yang dijadikan target virus pada sistem biasanya meliputi *Windows*, *System32*, *Startup*, *Application Data*. Lokasi ini paling sering digunakan karena menurut orang awam *file* pada lokasi tidak boleh dihapus dan hampir semua *file* yang ada merupakan *file* penting dan dapat mengalami kerusakan, hal ini dimanfaatkan oleh virus untuk melindungi dirinya.



Gambar 2. Virus Menggandakan Diri Ke Sistem

Pada gambar 2 di atas yang ditunjuk dengan tanda panah berwarna merah, menunjukkan virus yang diuji oleh penulis telah menggandakan diri ke sistem yang diinfeksinya. Setelah virus menggandakan diri, virus akan mengatur *registry* untuk mengaktifkan virus ketika sistem aktif dan juga memblokir setiap fungsi *Windows* yang dapat mengancam keberadaan virus ini. Selanjutnya virus akan mengaktifkan *file* induk dari virus yang telah ada pada sistem yang diinfeksi.

2. Melakukan Pengaturan Registry

Virus yang berjalan pada sistem operasi Windows tidak dapat lepas dari bantuan registry yang dapat membuat virus tersebut mampu memiliki pertahanan diri sehingga sulit untuk dimusnahkan. Registry dimanfaatkan oleh virus sebagai salah satu benteng pertahanan yang dapat menlindungi dirinya dari berbagai serangan-serangan yang dapat membuat dirinya musnah dari komputer yang telah terinfeksi.

3. Melakukan Pengaktifan Virus Pada Sistem

Jika virus telah melakukan penggandaan di sistem komputer, maka virus tersebut akan mengaktifkan hasil penggandaannya yang telah berada di sistem, sehingga meskipun *Flashdisk* atau *Flashdrive* dan juga media penyimpanan lain yang digunakan sebagai suatu sarana penyebaran virus tersebut dilepas, virus akan tetap aktif.

Gambar 3. Tampilan Virus Yang Aktif Pada Sistem

Pada gambar 4.2 di atas menampilkan bentuk virus yang telah aktif pada sistem yang diinfeksinya. Output dari virus tersebut tidak bisa ditutup dengan cara biasa karna tidak menyediakan *controlbox* pada *Form Header*. Tampilan dari output virus-pun juga akan selalu berada paling atas dari semua *Window* yang dibuka oleh *user*, sehingga akan menghalangi *user* untuk beraktivitas sekaligus memberitahukan kepada pengguna komputer yang terinfeksi tentang keberadaan virus ini.

4. Teknik Penyebaran

Ada banyak teknik penyebaran yang dilakukan oleh virus, berikut adalah beberapa teknik penyebaran yang biasa dilakukan oleh virus terhadap sistem.

a. Membaca *Address Bar* pada Windows Explorer

Teknik ini sangat baik selain proses penyebaran yang cepat dan juga tidak memerlukan suatu teknik pencarian *file*. Hal itu dikarenakan user telah memberikan informasi lokasi *file* yang dianggap penting dengan cara membuka folder tersebut menggunakan Windows Explorer yang selanjutnya user akan menjalankan *file*. Virus akan mendapatkan lokasi yang dimaksud dan langsung menggandakan diri ke dalamnya. Biasanya penamaan file dari hasil penggandaan virus diambil dari nama subfolder yang sedang terbuka.

b. Membaca Folder atau Sub Folder

Cara penggandaan yang satu ini sangat memakan banyak waktu untuk proses penyebaran. Tapi jika penyebaran berhasil, berdasarkan subfolder untuk satu partisi sistem saja dapat menghasilkan ribuan, apabila *user* menggunakan *Multi Operating System*

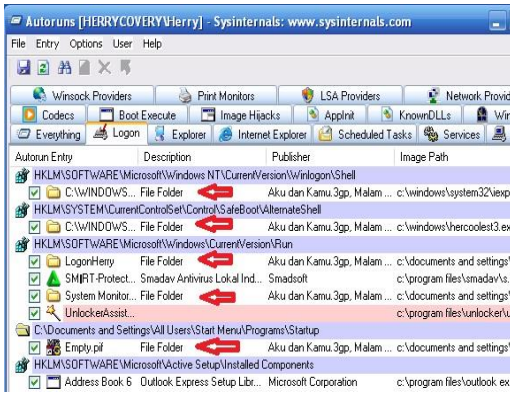
di komputernya, akan mengakibatkan kerusakan sistem lebih parah lagi.

5. Rekayasa Teknik Penyebaran

Setelah virus tersebut melakukan penggandaan ke sistem dan mengaktifkan diri, virus akan mengubah registry, dan setelah itu barulah virus tersebut melakukan penyebaran pada setiap lokasi yang sedang dibuka oleh *user* melalui *Windows Explorer*, kemudian setelah itu virus akan melakukan perusakan serta memodifikasi file yang dijadikan target.

6. Hasil Infeksi Virus Pada Sistem

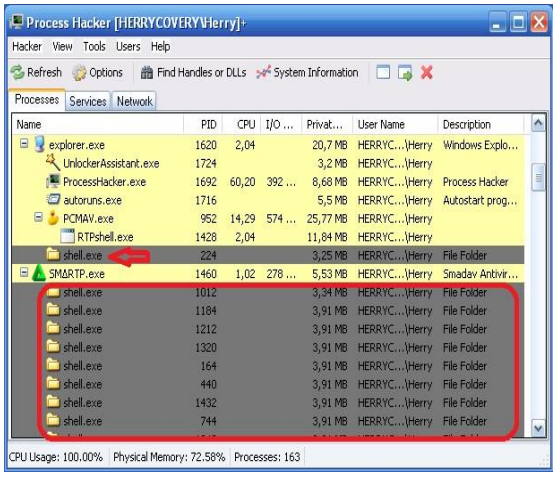
Virus melakukan infeksi dan memasuki sistem bertujuan agar virus bisa menguasai sistem yang telah diinfeksinya. Hasil infeksi virus pada sistem setelah melakukan penggandaan diri bisa dilihat pada gambar 4.3 di bawah ini. Penamaan dari *file* virus serupa dengan nama *file-file* sistem. Hal ini bertujuan agar membuat *user* ragu ingin menghapus atau menonaktifkan virus tersebut.



Gambar 4. Infeksi Virus Pada Sistem

Pada gambar 4 di atas memperlihatkan keberadaan virus yang telah memasuki sistem dan mengatur *registry* pada sebuah komputer. Setelah melakukan pengaktifan diri, pada sistem, virus akan melakukan rutinitas untuk memonitor segala aktivitas *user* dalam menggunakan *Windows Explorer*.

Pada gambar 5 di bawah ini merupakan proses virus yang aktif pada sistem yang telah diinfeksi. Proses virus yang aktif berada pada lingkaran dan tanda panah yang berwarna merah.

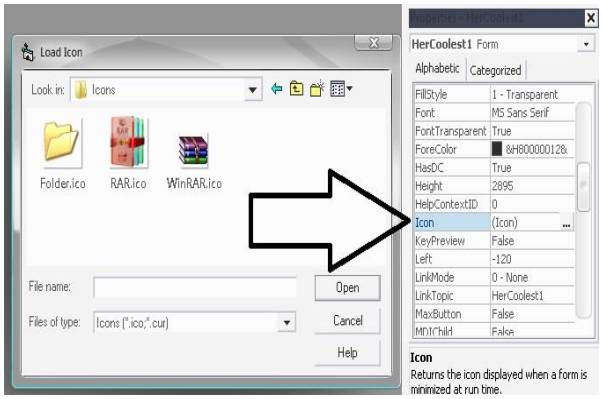


Gambar 5. Proses Virus Yang Telah Aktif Pada Sistem

7. Tampilan Infeksi Virus Pada File

Setelah virus aktif, virus akan memonitor segala aktivitas *user* dengan membaca *Address Bar*, *Caption* pada setiap aplikasi atau program yang dijalankan oleh *user*. Apabila yang sedang diakses oleh *user* merupakan target dari virus, maka virus akan memodifikasi atribut *file* tersebut terlebih dahulu, setelah itu virus akan mengganti *file user* tersebut dengan *file* virus yang telah digandakan pada lokasi tersebut. Kemudian apabila *user* ingin mengakses *file* tersebut untuk yang akan datang, maka yang akan diakses dan dieksekusi oleh *user* tersebut adalah *file* virus itu sendiri.

merupakan salah satu contoh dari tampilan infeksi virus yang telah penulis coba (uji program sebelumnya untuk melihat hasil infeksi dari virus dan membuktikan berhasil atau tidaknya virus ini dapat bekerja pada sistem operasi Windows sebagaimana tujuan awal pembuatan virus ini. Hasil atau tampilan dari infeksi virus bisa diganti sesuai keinginan, dengan cara mengganti objek *Properties* pada *Form Design*, di mana objek yang diganti adalah *file* icon. Pilih gambar atau icon dengan cara mengklik objek icon pada *Properties*, kemudian akan muncul jendela *Load Icon*. Pada jendela tersebut *browse* atau carilah gambar (icon) yang diinginkan seperti pada gambar 4.6 di bawah ini.



Gambar 7. Jendela Load Icon Visual Basic 6.0

8. Cara Penanggulangan

Untuk menanggulangi serangan virus secara umum, baik itu *trojan*, *worm* dan jenis *malware* lainnya, berikut ini pembahasan cara-cara menanggulangi *malware* baik sebelum terinfeksi dan juga setelah terinfeksi. Akan tetapi perlu diketahui bahwa virus yang dibuat oleh penulis ini masih memiliki kelemahan antara lain, yaitu masih mudah terdeteksi oleh beberapa Antivirus Internasional atau biasa disebut Antivirus import, khususnya Antivirus yang selalu diupdate rutin oleh *user*. Kelemahan lainnya merupakan teknik penyebarannya yang masih sederhana, yaitu hanya menangkap aktivitas dari *user* dengan menggunakan kode *Get Files* pada *Windows Explorer*.

9. Sebelum Terinfeksi

Berikut adalah beberapa langkah-langkah yang dapat dilakukan untuk pencegahan serangan *malware* sebelum komputer atau bagian-bagian dari komputer terinfeksi:

a. Gunakan Antivirus yang dipercaya dengan update terbaru. Apapun merek dari Antivirus yang dimiliki asalkan selalu diupdate secara rutin dan selalu menyalakan *Protection* pada Antivirus tersebut. Apabila ada *file* yang dicurigai harap segera mengirim contoh *file* tersebut ke pengembang Antivirus yang digunakan.

b. Selalu memindai (*scan*) setiap media penyimpanan eksternal yang akan digunakan, misalnya penggunaan USB Flashdrive atau Flashdisk dan sebagainya. Hal ini memang agak merepotkan, tetapi jika *Protection* Antivirus yang digunakan sedang dalam keadaan aktif, maka langkah ke dua ini dapat dilewatkan.
akan digunakan.

e. Apabila tidak ada Antivirus yang mendeteksi, maka biasakan menggunakan teknik untuk menghindari *malware* secara umum agar *malware* tidak ada yang bisa berjalan secara otomatis pada sistem yang kita gunakan. Penyebaran *malware* di Indonesia paling rentan adalah pada media

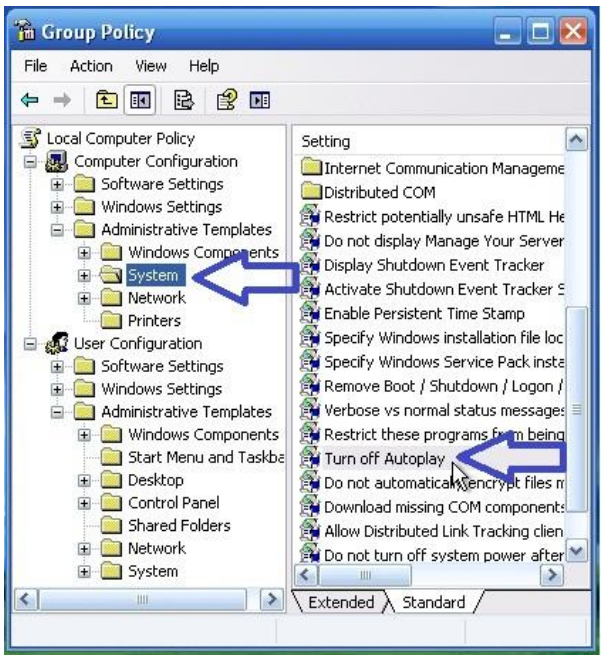
Pada *Windows XP* untuk menonaktifkan *Autoplay* bisa tekan pada *keyboard* tombol *Windows* + R. Maka akan muncul *Window*

c. Jika terhubung langsung ke Internet cobalah untuk menggunakan Antivirus yang sekaligus berfungsi ganda dengan fitur *Internet Security*. Dengan adanya *Internet Security*, Antivirus tersebut akan melindungi kita dari *website* berbahaya yang memuat *malware* pada halamannya.

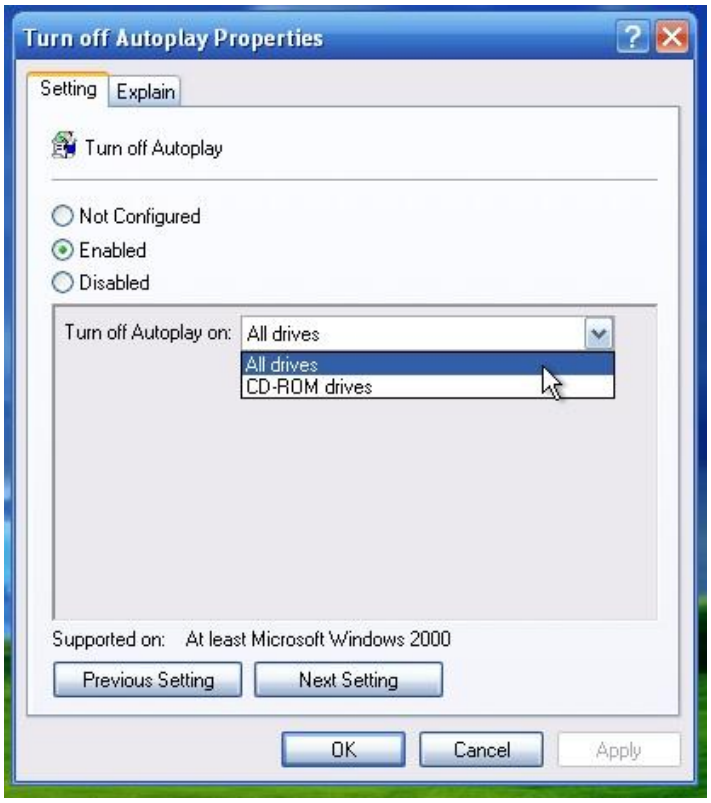
d. Apabila ingin mengujicobakan sebuah aplikasi yang tidak dipercaya atau bukan dari situs-situs resmi, harap gunakan aplikasi yang menyediakan area virtual pada sistem, sehingga ketika kita menjalankan sebuah aplikasi yang bermasalah atau telah diinfeksi oleh virus, maka sistem utama kita tidak akan bermasalah dan aman dari infeksi virus. Pada beberapa Antivirus Internasional telah menggunakan fitur *Sandbox* atau *Safe Run* yang dikhususkan untuk mengujicobakan aman atau tidaknya software-software yang

USB. Agar *malware* tidak memasuki sistem kita melalui USB, berikut teknik menghindari *malware* yang menyusup melalui fitur *Autoplay* bawaan *Windows* pada Windows XP dan Windows 7:

dialog *Run*. Ketikkan : GPEDIT.MSC pada *textbox* tersebut dan kemudian tekan *Enter* pada *Keyboard*.

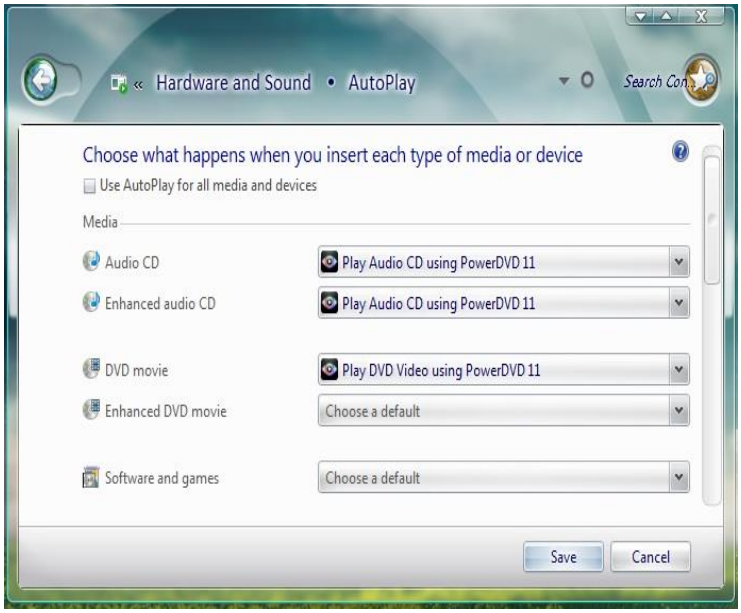


Gambar 8. Turn Off Autoplay Pada Windows XP



Gambar 9. Turn Off Autoplay Properties

Setelah jendela dialog seperti pada gambar 9 di atas muncul, pilih opsi *Enabled* kemudian pilih *Turn off Autoplay on : All Drives*. Untuk selanjunya pada *User Configuration* lakukan dengan cara yang sama. Pada *Windows 7* untuk menonaktifkan *Autoplay* bisa langsung menuju *Control Panel* dan pilih *Hardware and Sound*, kemudian pilih *Autoplay.*



Gambar 10. Turn Off Autoplay Pada Windows 7

10. Setelah Terinfeksi

Berikut adalah beberapa langkah yang dapat dilakukan pada saat komputer atau bagian-bagian dari komputer telah terinfeksi:

a. Deteksi dan tentukan di mana letak sumber virus tersebut, dan ada baiknya memutuskan sambungan ke jaringan atau internet terlebih dahulu.
b. Identifikasi dan klasifikasi jenis virus yang menyerang sistem dengan cara:
    1. Gejala yang timbul, misal: pesan, file yang *corrupt* (rusak), *file* yang hilang, dan gejala aneh lainnya atau yang tidak biasanya terjadi.
    2. Kirimkan file virus yang ditemukan dan telah banyak menyebar pada sistem, kemudian update Antivirus yang digunakan segera agar mendapatkan pembaharuan *database* yang mampu mengenal *malware-malware* baru yang banyak beredar. Setelah melakukan *update*, pindai (*scan*) partisi sistem untuk melumpuhkan virus yang aktif. Apabila masih belum dideteksi oleh Antivirus tersebut, tunggu beberapa hari lagi. Biasanya Antivirus Internasional mampu memperbaharui *database* pengenal virus setiap hari dikarenakan banyaknya jumlah *malware* yang beredar tiap harinya secara global.
c. Jika Antivirus telah diperbaharui dan tidak berhasil memusnahkannya, maka carilah *Removal* khusus untuk virus tersebut sesuai dengan nama pendeteksiannya di situs-situs yang memberikan informasi perkembangan virus.
d. Jika semua hal di atas tidak berhasil, maka cara terakhir adalah dengan memformat partisi sistem pada komputer tersebut dan kemudian menginstal ulang komputer yang terkena infeksi tersebut.
e. Cara manual dalam membersihkan virus, bisa dengan menggunakan *software-software tools* sejenis *Task Manager*, namun kita tidak akan selalu bisa menggunakan *Task Manager* dikarenakan pada beberapa *malware* ada yang memiliki *self-defence* sehingga tidak bisa menggunakan *Task Manager* dan beberapa *Tools* yang disediakan oleh *Windows*. Pilihan lain untuk menggunakan beberapa *software tools* lainnya seperti: *Process Hacker, Process Explorer, Autoruns, Unlocker,* dan lain-lain.

KESIMPULAN

Dengan teknik ini, kita bisa mengetahui cara kerja virus atau aktivitas virus secara umum yang segala aksinya ditentukan pada penulisan kode di *Event Form Load* dengan mengubah pengatuan *Registry* dan merusak sistem pada komputer dan memodifikasi *file-file* yang dijadikan target serangan oleh virus dan dapat mempertahankan diri dengan selalu mengaktifkan aplikasi. Disamping itu, kita dapat mengambil sisi positifnya, yaitu kita bisa mempelajari cara menghindari serangan *malware* agar tidak memasuki sistem komputer kita, dan juga merupakan suatu dorongan kepada para pengembang Antivirus Indonesia agar bisa meningkatkan kualitas produk mereka masing-masing.

DAFTAR PUSTAKA

Community, eWolf, 2011, **"Cara Paling Ampuh Membasmi Virus Komputer"**. Yogyakarta : MediaKom

Cohen, Frederick B, 1991, **"Fault Tolerant Software for Computer Virus Defense"**. Pittsburgh : ASP

Hendrawan, Leo, 2004, **"Virus Komputer: Sejarah Dan Perkembangannya"**. Bandung : Tugas Akhir

Hirin, A.M, 2010, **"Cara Praktis Membuat Antivirus Komputer"**. Jakarta : Mediakita

Hirin, A.M. & Anhar, 2009, **"Cara Praktis Membasmi Virus Ganas di Komputer"**. Jakarta : Mediakita

Hirin, A.M. & Anhar, 2012, **"Seri Kamu Pasti Bisa Membuat Virus Mematikan Disertai Source Codes"**. Jakarta : Prestasi Pustaka

Klang, Mathias, 2003, **"A Critical Look at the Regulation of Computer Virus"**, USA : Oxford University Press.

Kumar, H.Shravan, 2005, **"Seminar Report on Study of Viruses and Worms"**. I.I.T. Bombay: KReSIT. http://www.it.iitb.ac.in/~shravan/Seminar/report.pdf

Eric M. Hutchins, Michael J. Clopperty, Rohan M. Amin, Ph.D, 2010. **"Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"**, Lockheed Martin Corporation

Master.com, 2011. **"Membuat Dan Membasmi Virus Komputer"**. Jakarta : Kunci Aksara

Prabhat K. Singh, Arun Lakhotia, 2002. **"Analysis and Detection of Computer Viruses and Worms : An Annotated Bibliography",** USA, ACM SIGPLAN Notices

Sadeli, Muhammad, 2009, **"Membuat Sendiri Kontrol ActiveX dengan Menggunakan Visual Basic 6.0"**. Palembang : Maxikom

http://www.pusatgratis.com/tutorial/security/alasan-pembuat-virus.html

http://www.pusatgratis.com/tutorial/security/kemampuan-dasar-virus.html

http://www.pusatgratis.com/tutorial/security/mengenal-virus-bagian-1.html

http://www.pusatgratis.com/tutorial/security/mengenal-virus-bagian-2.html

http://www.pusatgratis.com/tutorial/security/pengertian-virus.html