

Mengamankan Komputer dengan Meminimalisir Serangan **VIRUS** tanpa Anti Virus

Moch.David Fachrudy

dav_idpunk@yahoo.com

Lisensi Dokumen:

Copyright © 2003-2007 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

Sehubungan dengan kekreatifitasan dan pro aktifnya bangsa Indonesia kita dalam membuat virus yang sangat bervariasi, dan banyaknya laporan-laporan para pengguna komputer yang merasa terganggu dengan adanya virus saat ini yang telah semakin canggih bahkan lebih canggih dari mesin scanner antivirus terkenal yang mereka pakai sekalipun. Maka dari itulah saya terdorong untuk menulis tutorial sederhana ini berharap dapat membantu kalayak ramai yang masih suka memakai anti virus tapi malas mengupdatenya..., dan dalam rangka mengumpulkan pundi-pundi pahala tentunya he..he...99x, lumayanlah buat bekal nanti klo udah di sono??? Daripada buat virus, "DOSA" merugikan orang lain!!!... lebih baik kita buat sesuatu yang bermanfaat :-). Yup!!!... Nah dari pada saya kebanyakan ngelantur, lebih baik kita lanjutkan kisah berikutnya... *simak baik-baik...*

Sekilas tentang VIRUS....

- Virus kebanyakan selalu menyamarkan diri dengan membuat ikonnya seperti   file-file umum yang sering kita lihat dan gunakan supaya kita terkecoh. Sebagai contoh, VIRUS, paling sering menggunakan ikon *file folder (kuning)* dan *file MSWord* karena memang selama ini sangat efektif untuk mengecoh calon korban.

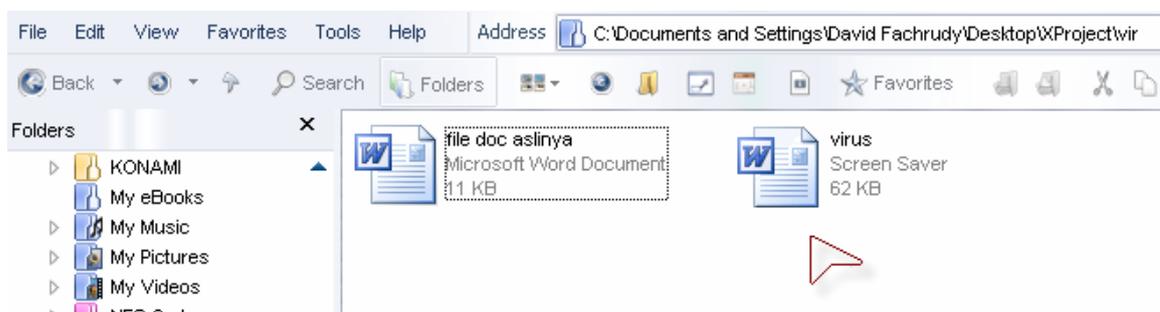
- Akan tetapi bukan berarti hanya terpatok pada dua ikon file tersebut, bisa juga dalam bentuk yang lainnya seperti file gambar.jpg, file text.txt, game flash.exe, file installer.exe/.msi dan lain-lain, pokoknya pinter-pinternya bagaimana cara virus itu dapat mengecoh kita dengan berbagai macam godaannya, jadi berhati-hati sajalah.

I. Langkah Pertamanya adalah:

“Gantilah bentuk icon-icon yang sering di tiru oleh virus tersebut atau icon file lain yang kemungkinan dapat dimanfaatkan virus untuk mengecoh kita.”

Maksudnya adalah agar kita bisa tau lebih dini apabila ada virus yang baru saja masuk dikomputer kita yang biasanya datang dari flashdisk atau peralatan disk removable yang lainnya. Karena akan sangat kelihatan berbeda di tampilan explorer komputer kita nantinya. Sehingga dapat mencegah kita untuk tidak mengaktifkan virus tersebut dan kita bisa langsung menghapusnya sebelum menyebar atau menjangkiti komputer kita.

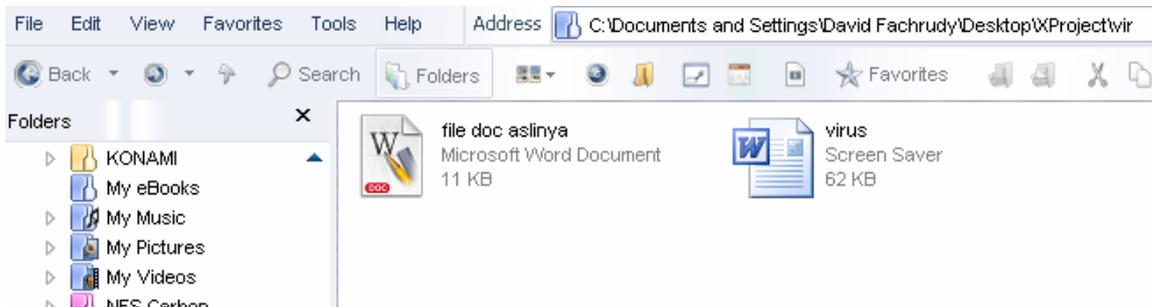
Dibawah ini adalah screenshot tampilan di explorer saat kita belum merubah bentuk ikon file dokumen word



Screenshot Sebelum icon diganti

Diatas dapat kita lihat bahwa tidak ada perbedaan antara file VIRUS dan file asli, jadi mungkin saja kita bisa terkecoh untuk me'clicknya / mengaktifkannya karena kita berfikir itu adalah file word.

Sedangkan dibawah ini adalah screenshot tampilan di explorer setelah kita mengganti/merubah bentuk ikon file dokumen word.

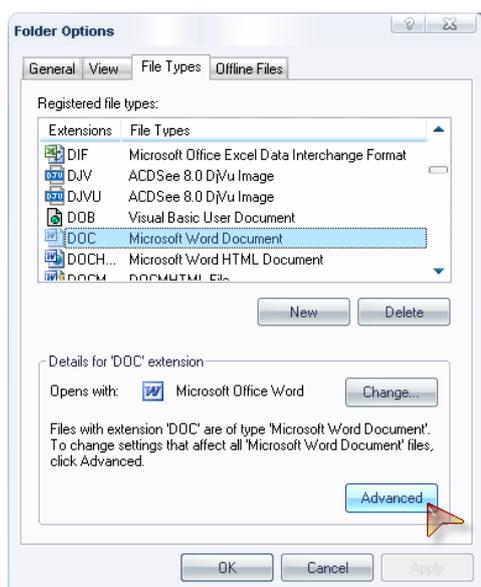


Screenshot Setelah icon diganti

Diatas dapat kita lihat perbedaan mencolok antara file VIRUS dan file asli. Dikarenakan file document word (*.doc & *.rtf) telah diganti dengan icon yang lain maka apabila kita menemui file yang iconnya masih seperti yang sebelum diganti maka itu adalah virus, dan sebaiknya langsung dihapus saja karena sudah dipastikan itu virus.

- Cara mengganti bentuk icon-nya adalah:

Masuklah “**Explorer-Tools-Folder Options...**” atau dapat melalui “**Control Panel-Folder Options...**”



Lalu masuklah ke tab “**File Types**” trus di kolom bawahnya itu kamu dapat melihat semua jenis ekstensi file dan icon-iconnya.

Untuk mengganti icon pilih salah satu ekstensi file yang mau diganti, misalnya ekstensi ***.doc** dan ***.rtf**, keduanya adalah file word dokumen yang sering ditiru virus, maka saran saya sebaiknya diganti saja keduanya satu persatu.

Click tombol “**Advanced**”, lalu click “Change Icon...” pilih atau cari file icon melalui tombol “Browse...” yang berekstensi ***.ico**, ***.icl**, ***.exe**, dan ***.dll** yang mengandung icon sesuai selera anda, setelah itu click “**OK**” lalu “**Close**”.

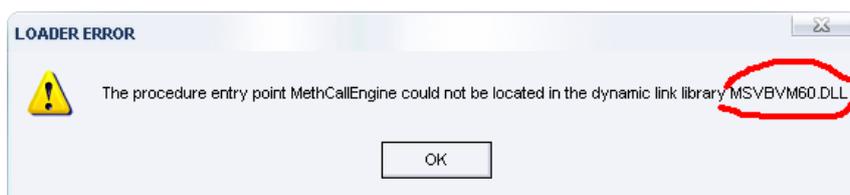
Ulangi langkah2 diatas untuk file: ***.rtf**, **Folder** dan **File Folder** karena file inilah yang paling sering dijiplak virus. Khusus untuk Icon Folder kadang kurang efektif apabila digantinya lewat cara diatas, jadi saran saya instal-lah suatu Software yang dapat merubah tampilan bentuk icon folder seperti: **iColor Folder**, **Pack Vista Inspirat**, **StyleXP**, **TuneUp Utilities**, dan masih banyak lagi software sejenis yang lainnya,

Untuk cara lebih sulit bisa melalui via registri atau merubah langsung resource iconnya di explorer.exe dan di shell32.dll menggunakan software resource compiler seperti “ResHacker”, XNResource, dll. Dan untuk mengetahui caranya lebih lanjut request aja ke dav_idpunk@yahoo.com.

II. Langkah Kedua:

1. Faktanya adalah....

- Sekitar 85% virus di Indonesia, dan 65% virus dari Luar Negeri menggunakan bahasa pemrograman “*Visual Basic*”. Sedangkan Program atau virus yang dibuat menggunakan bahasa pemrograman Visual Basic untuk dapat berjalan di Sistem Operasi Windows akan selalu membutuhkan suatu file modul yang bernama “*msvbvm60.dll*” yang letaknya di direktori “*C:\WINDOWS\system32*”. Jadi apabila file tersebut tidak ada, maka dari ke 85% virus dari Indonesia, dan 65% virus dari Luar Negeri tersebut tidak akan bisa berjalan, akan tetapi resikonya adalah apabila ada aplikasi yang bukan virus yang juga dibuat dengan bahasa pemrograman Visual Basic juga akan lumpuh di komputer tersebut, dan akan menampilkan pesan error seperti dibawah ini.



Kadang juga seperti dibawah ini...



Pesan error diatas muncul dikarenakan adanya sebuah aplikasi Visual Basic yang gagal di eksekusi dikarenakan file modul msvbvm60.dll yang dibutuhkannya tidak ada atau tidak ditemukan.

Jadi maksud saya adalah sebaiknya file msvbvm60.dll direname saja, dan apabila ada aplikasi bukan virus yang akan anda jalankan error dan menampilkan pesan error seperti diatas, maka rename kembali file msvbvm60.dll dan setelah selesai rename lagi dengan nama lain. Jangan berfikir hal ini merepotkan, sebab saat ini jarang sekali ada aplikasi resmi yang masih menggunakan bahasa pemrograman visual basic.

- Cara me-rename file msvbvm60.dll dengan cepat:

Terlebih dahulu buatlah file *vbren.bat* dan *vbfix.bat* :

- ✓ Buka *notepad.exe* dan ketikkan :

```
ren C:\windows\system32\msvbvm60.dll 1111msvbvm60.dll
```

- ✓ lalu save dengan nama: “**vbren.bat**” dan disimpan di direktori “C:\windows\”,,
- ✓ jika sudah di simpan, buatlah satu lagi tapi isinya :

```
ren C:\windows\system32\1111msvbvm60.dll msvbvm60.dll
```

- ✓ lalu save dengan nama: “**vbfix.bat**” dan disimpan juga di direktori “C:\window\”

Setelah file *vbren.bat* dan *vbfix.bat* selesai dibuat, maka apabila anda ingin merename file msvbvm60.dll anda tinggal membuka “**Start menu – RUN**” atau lebih cepatnya pencet

tombol “**Win+R**” dan ketikkan **vbren** lalu **Enter**, maka file *msvbvm60.dll* tersebut namanya akan berubah menjadi ***1111msvbvm60.dll***

Dan apabila anda ingin mengembalikan namanya seperti semula, buka kembali RUN atau pencet tombol “**Win+R**” dan ketikkan **vbfix** lalu **Enter**, maka file *msvbvm60.dll* tersebut namanya akan kembali menjadi ***msvbvm60.dll***

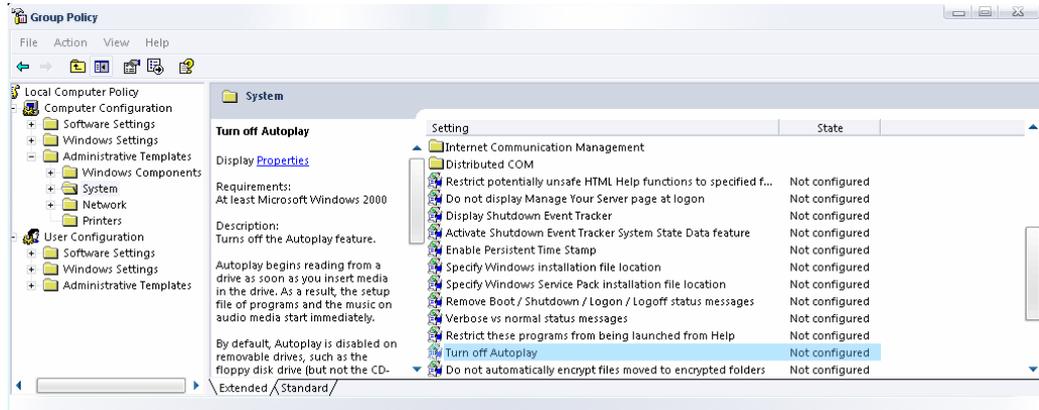
III. Langkah Ketiga:

Pada masa kejayaan virus yang dirajai oleh virus brontok dkk, dan beberapa virus lain sejenisnya, virus tersebut hanya dapat menjangkiti komputer apabila diaktifkan dengan cara manual saja (via click2x, click kanan-open, atau enter) akan tetapi saat ini virus-virus tertentu yang menyebar lewat removable disk seperti USB Flash disk, memory card, dan lain-lain dapat mengaktifkan dirinya secara otomatis untuk menjangkiti komputer kita. Hal tersebut disebabkan karena virus-virus tersebut menggunakan fasilitas “*autorun*” pada Sistem Operasi Windows, yaitu dengan menambahkan file *autorun.inf* dan *folder.htt* di dalam peralatan removable agar apabila peralatan removable tersebut saat dikoneksikan dengan komputer, virus yang ada didalamnya bisa langsung menyerang secara otomatis tanpa harus menunggu untuk diaktifkan oleh user, seperti halnya virus-virus terdahulu.

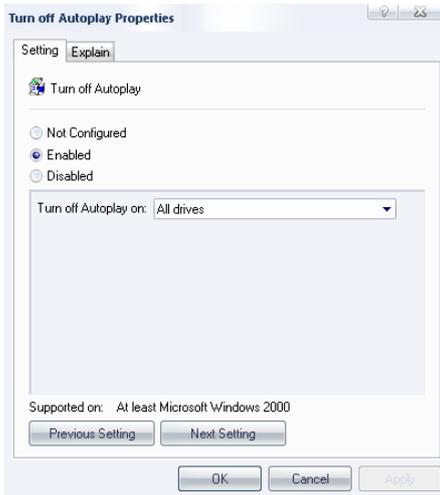
Jadi untuk menghindari virus-virus semacam itu kita harus mematikan fungsi *autorun* pada system operasi windows.

- Cara mematikan fungsi autorun pada windows:

- Buka RUN lalu ketikkan “*gpedit.msc*” untuk membuka “*Group Policy*”.
- Buka pada bagian “*Computer Configuration - Administrative Templates - System*”.



- Lalu pada bagian kanan windows di tab “setting” cari tulisan “Turn off Autoplay” dan click2x / enter, akan muncul tampilan seperti dibawah ini.



- Beri tanda cek pada pilihan “Enable”, lalu dibawahnya pada bagian “Turn off Autoplay on” click “All Drive” pada pilihannya. Untuk lebih jelasnya lihat gambar disamping.
- Setelah tadi kita menyeting pada bagian “Computer Configuration” selanjutnya pada bagian “User Configuration” (“User Configuration - Administrative Templates – System”) juga harus diseting dengan cara yang sama seperti langkah-langkah diatas.
- Dengan begitu apabila ada virus yang memanfaatkan fungsi autorun pada windows untuk masuk kekomputer dapat tercegah dan kita bisa menghapusnya sebelum menyerang.

Nb:

Kalau menurut saya sebaiknya kalau bisa kita jangan terlalu bergantung pada anti virus ataupun aplikasi2 instan yang lain yang sebenarnya masih bisa dilakukan secara manual, kecuali memang sangat diperlukan. Jadilah pintar dengan bekerja keras agar kita tidak selalu menjadi korban dari orang yang lebih pintar dari kita.

Nb lagi:

Sebelumnya saya beritahukan bahwa, saya yakin suatu saat seiring berkembangnya teknologi dan metode-metode penyebaran virus yang akan datang akan membuat tutorial ini “*basi*” (tidak berguna). Sebab para pembuat virus juga pasti akan terus belajar untuk menemukan metode-metode penyebarannya yang baru.

Nb (satu lagi ya...):

Saya bukan bermaksud sok pintar menulis ini, (wong nilai IP saya aja jelek2, suer!!), ya... Cuma berharap semoga bisa berguna. Dan apabila ada yang mempunyai cara lebih bagus dan murah tolong kirim ke e-mailku ya dav_idpunk@yahoo.com

Nb: (Nb terakhir ni! Sumpe dech!!!...) ☺

Untuk para senior yang ahli komputer mohon jangan mengejek, maklum newbie. akan lebih saya terima kalau situ mau ngajarin saya trik-trik bagus berkomputer yang belum banyak diketahui orang.

“Nambah:”...he..he..1000x☺

Gak Jadi ah!...

Biografi Penulis



Moch. David Fachrudy, lahir dan besar dari kecil hingga lulus SMU di kota NewYork (Ah...bohong!). Madiun (yyuk..!). Lalu setelah lulus dari *SMUN I Dagangan* dan tidak diijinkan lagi sekolah disana, mulailah hijrah ke kota Pelajar Jogjakarta untuk melanjutkan perjuangan, dan hingga saat ini. Masih berstatus kuliah S1 di Universitas IST.AKPRIND Yogyakarta jurusan ILMU KOMPUTER. Hobi main gitar dan tidur siang so malemnya melexs (nglowo). Maaf tidak mempunyai prestasi apa-apa untuk dituliskan disini, jadi cukup sampai disini sajalah.