

Tips menghindari malware

Malware (virus, trojan, script, worm, spyware, etc) tidak hanya tersebar dari Internet, tapi dapat juga tersebar dari media penyimpanan offline (disket, CD, DVD, UFD (Universal Flash Disk), etc), bahkan peranan media penyimpanan ini sangat berperan dalam penyebaran malware di negeri kita. Tulisan ini merupakan lanjutan dari tulisan penulis (YKS) yang berjudul **Tips untuk Pengguna Warnet** (<http://myks.wordpress.com/2008/02/06/tips-untuk-pengguna-warnet/>). Dengan tulisan ini diharapkan kita semua dapat semakin mahir dalam menghindari malware yang mencoba menyusup ke komputer kita sehingga komputer kita bisa selamat dari bahaya malware.

K. Mencegah malware dari sisi software

Terdapat beberapa tips untuk selamat dari ancaman malware dari media penyimpanan pada sistem operasi Microsoft Windows*, tetapi penulis hanya memberikan tips yang mudah yang bisa diterapkan oleh siapapun. Jadi, Anda tidak perlu harus sangat mengerti seluk-beluk komputer, Internet, atau teknologi informasi secara detil untuk dapat menjalankan tips berikut ini ;)

Berikut ini cara penting untuk dapat mencegah malware dari komputer Anda :

1. Install Anti Virus

Software anti virus merupakan satu benteng cukup penting untuk dapat menghalau bahaya malware, komputer yang sudah terinstall suatu anti virus adalah lebih baik dan lebih aman daripada komputer yang tidak terinstall anti virus. Untuk memilih anti virus, pilihlah anti virus yang handal dan cepat, dan jangan memilih anti virus yang membebani sistem komputer Anda. Rekomendasi penulis tentang hal ini secara global adalah ESET NOD32 (anti virus komersil yang handal dan paling cepat, free trial untuk satu bulan). Sedangkan untuk pencegahan ancaman virus-virus lokal, penulis merekomendasikan PCMAV (PC Media Anti Virus), tapi penulis tidak merekomendasikan majalahnya hehehe (loh kok!?).

2. Update Anti Virus

Malware-malware baru akan terus bermunculan, karena itu komputer Anda tidak hanya cukup terinstall anti virus, melainkan Anda juga perlu rajin update anti virus yang Anda gunakan, terutama dalam database virus anti virus itu.

L. Mencegah malware dari sisi brainware

Sehebat-hebatnya software tetap saja buatan manusia, dan buatan manusia itu tidak ada yang sempurna, sehingga jika Anda hanya mengandalkan software untuk mencegah malware, maka Anda telah mengandalkan sesuatu yang mudah rapuh yang hal itu akan dapat rapuh kapan saja saat kelemahan itu muncul atau saat Anda melakukan kesalahan. Jadi bagaimana caranya supaya kita dapat mencegah malware secara optimal?

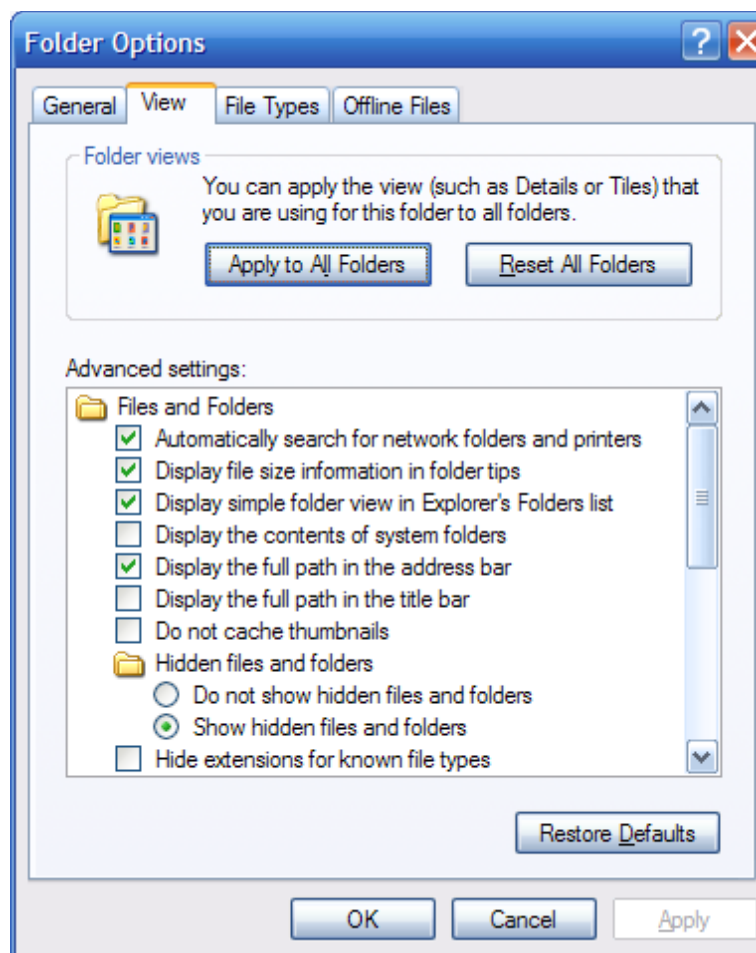
Cara terpenting dan terbaik dalam mencegah malware adalah mencegah hal itu dari sisi brainware / manusia, yaitu manusia itulah yang harus lebih berhati-hati dalam menggunakan komputer, terutama saat berselancar di Internet dan transfer data melalui media penyimpanan.

Cara dari sisi brainware inilah yang perlu dipelajari, diterapkan, dan disebarakan oleh setiap pengguna komputer agar dapat membuat komputernya lebih aman (terutama data-data) dan selamat dari bahaya malware.

Berikut ini adalah cara mencegah malware dari sisi brainware pada saat transfer data melalui media penyimpanan (sedangkan cara mencegah malware pada saat terkoneksi ke Internet sudah penulis jelaskan di [Tips untuk pengguna Warnet](#)), yaitu dari UFD (atau media portable lainnya) ke Hard Disk komputer atau sebaliknya :

1. Show Hidden Files

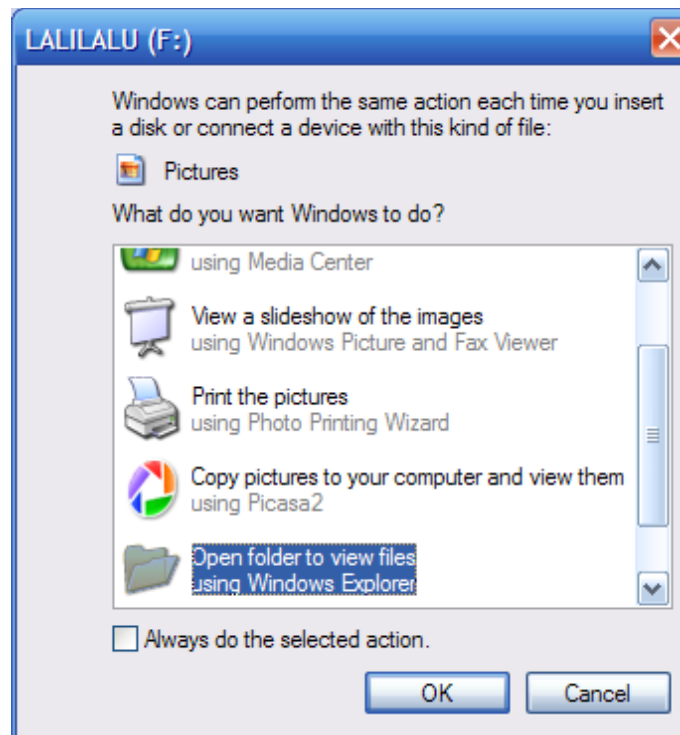
Selalu pastikan komputer Anda sudah menampilkan file-file yang tersembunyi. Untuk mengetahuinya adalah buka **Windows Explorer-->Tools-->Folder Options**. Lalu pada tab **View**, pastikan opsi **Show hidden files and folder** terpilih pada bagian Hidden Files and Folders. Dan pastikan pula **Hide extentions for known file types** tidak tercentang. Setelah itu tekan tombol OK.



Gambar L.1

2. Auto Run UFD

Biasanya saat kita memasukkan UFD ke komputer, sistem komputer kita akan menampilkan window seperti gambar berikut ini :



Gambar L.2

Untuk lebih aman, window seperti itu jangan sampai muncul lagi pada saat Anda memasukkan UFD ke komputer. Caranya adalah (pilih salah satu pilihan berikut) :

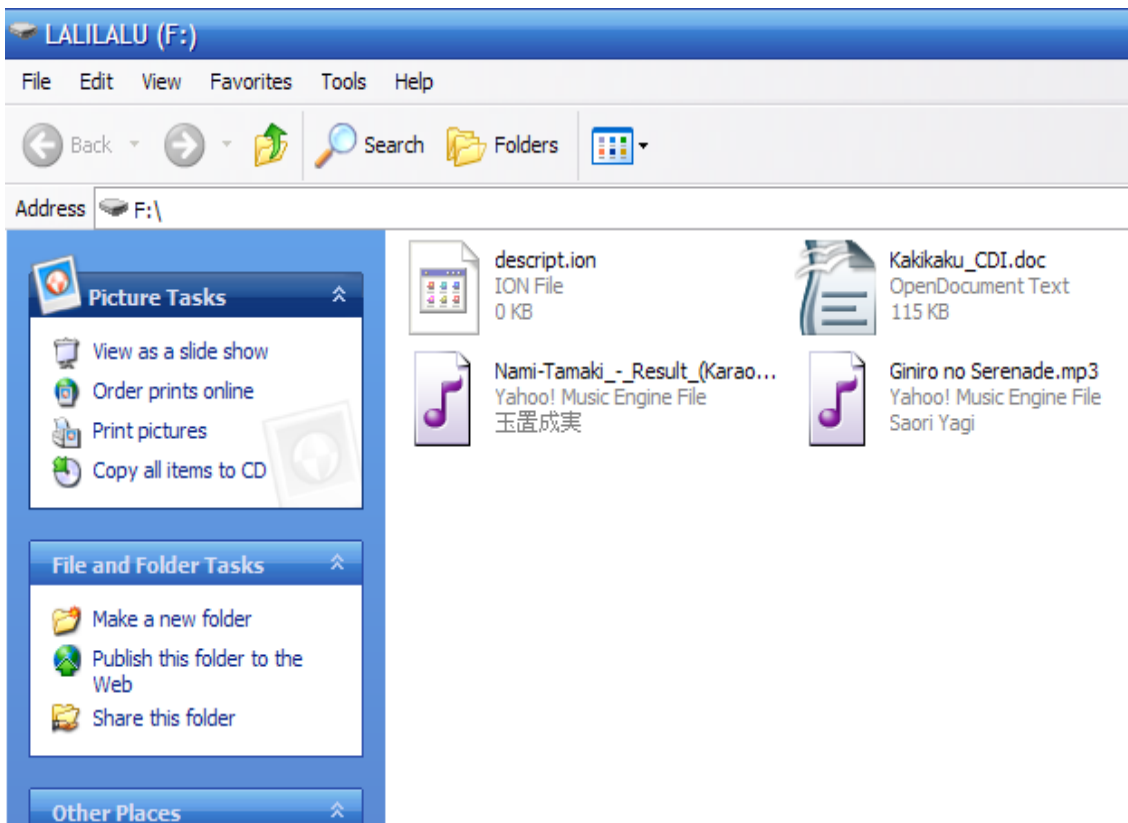
- Pilih **Open folder to view files**, beri tanda centang pada **Always to do the selected action**, lalu tekan tombol **OK** (cara yang dianjurkan).
- Pilih **Take no action**, beri tanda centang pada **Always to do the selected action**, lalu tekan tombol **OK**. (cara yang paling dianjurkan).
- Tekan tombol **shift** pada keyboard pada saat setiap kali Anda memasukkan UFD ke komputer Anda (tapi cara ini tidak begitu disarankan terutama bagi orang yang tidak mau repot atau sering lupa).

Manfaat utama dari tips ini adalah untuk mencegah autorun dari suatu malware jika UFD Anda terinfeksi suatu malware.

3. Perhatikan file yang aneh dan mencurigakan

Perhatikanlah file-file Anda yang ada di UFD, ingatlah file apa saja yang Anda masukkan sendiri di UFD Anda. Lalu jika Anda menemukan beberapa file aneh (yang anda tidak yakin file apa itu) setelah UFD Anda dimasukkan ke komputer lain (komputer teman, rental, warnet, kantor, dsb semuanya mempunyai kemungkinan sudah terinfeksi suatu malware), maka jangan sampai terbesit di pikiran Anda untuk membuka/menjalankan file aneh tersebut karena file tersebut bisa saja merupakan malware yang dapat memporak-porandakan sistem komputer dan data-data Anda.

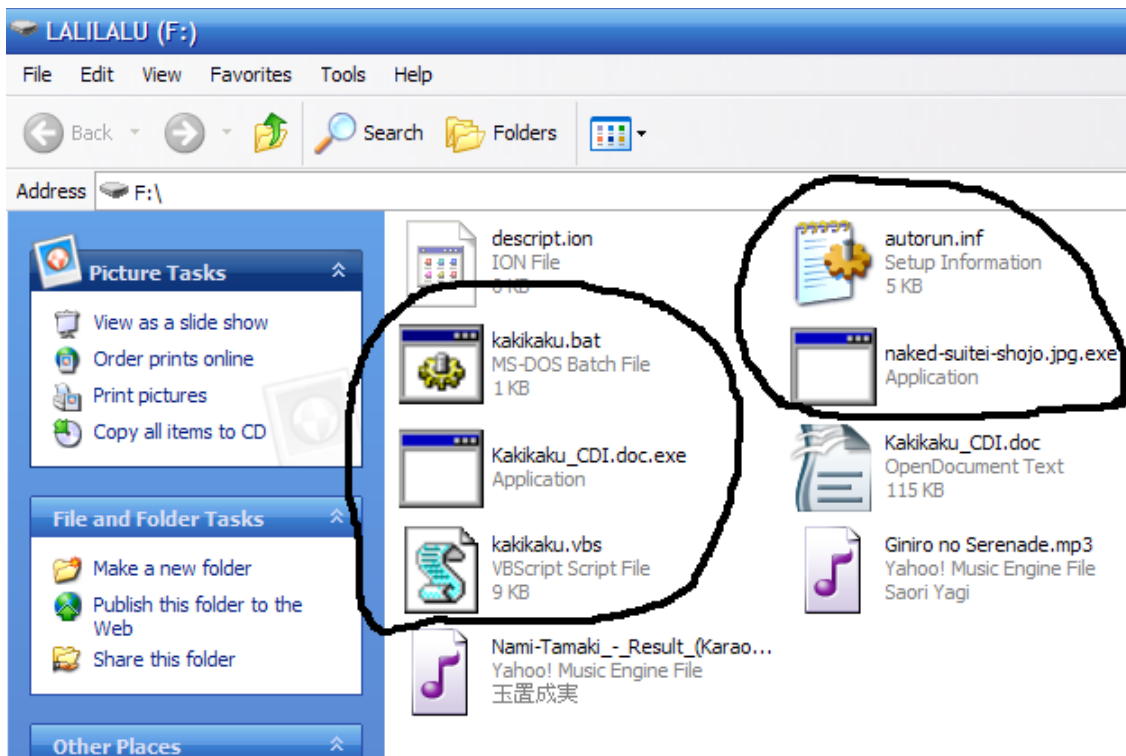
Sebagai contoh, UFD dengan label Lalilalu (teman dekat Kakikaku ^^) berikut ini masih dalam keadaan normal tanpa malware :



Gambar L.3

Pada gambar L.3 di atas, UFD Lalilalu itu berisi 4 file : **descript.ion**, **kakikaku_cdi.doc**, **Giniro no Serenade.mp3**, dan **Nami-Tamaki_-_Result_(Karaoke).mp3**. MP3 adalah file suara/musik, file doc adalah dokumen, sedangkan descript.ion adalah suatu file yang dibuat yang salah satu fungsinya adalah untuk menampung informasi tambahan untuk suatu file yang diinginkan. Descript.ion ini bisa berguna oleh sebagian orang dan bisa juga tidak berguna oleh sebagian yang lain, sehingga file descript.ion bisa dihapus (bagi yang tidak membutuhkannya) dan bukan file yang harus ada dalam setiap folder.

Lalu UFD Lalilalu itu beberapa kali dipakai untuk transfer data di komputer lain, terutama rental dan warnet. Ketika UFD Lalilalu kembali dimasukkan ke komputer pemilik UFD Lalilalu, ternyata ada beberapa file aneh seperti pada gambar di bawah ini :



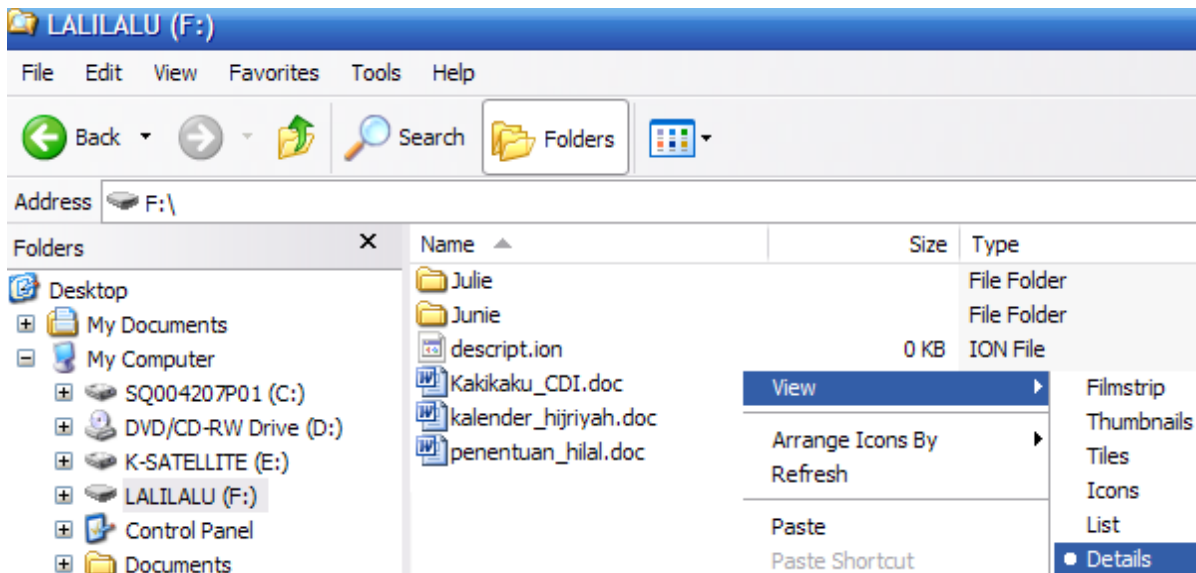
Gambar L.4

Ternyata UFD Lalilalu memiliki tambahan file aneh dan mencurigakan, yang pemiliknya tidak tahu tentang file itu atau tidak pernah memasukkan file-tersebut, yaitu : **autorun.inf**, **kakikaku.bat**, **naked-suitei-shojo.jpg.exe**, **Kakikaku_CDI_doc.exe**, dan **kakikaku.vbs**. Tidak usah penasaran dan jangan pernah terbesit di pikiran untuk mencoba membuka file-file aneh tersebut, tetapi hapus saja file-file aneh tersebut. Resiko jika nekad membuka file-file aneh tersebut adalah sistem komputer Anda kemungkinan besar akan terinfeksi malware dan data-data Anda bisa saja hilang karena file-file aneh itu kemungkinan besar (kata yang bisa diganti menjadi “pasti”) adalah malware.

Catatan : File yang memiliki extention .inf, .bat, .vbs, .exe pada dasarnya adalah netral, dan extentions tersebut tidak pasti merupakan suatu malware karena banyak pula file yang memiliki extention .inf, .bat, dan .exe yang bermanfaat dan sama sekali bukan malware. Maka patokannya adalah Anda harus waspada jika UFD Anda memiliki tambahan file aneh dan mencurigakan (misal : file dengan nama dokumen Anda tapi ekstensinya adalah exe), yang Anda tidak tahu tentang file itu atau Anda tidak pernah memasukkan file tersebut ke UFD tersebut.

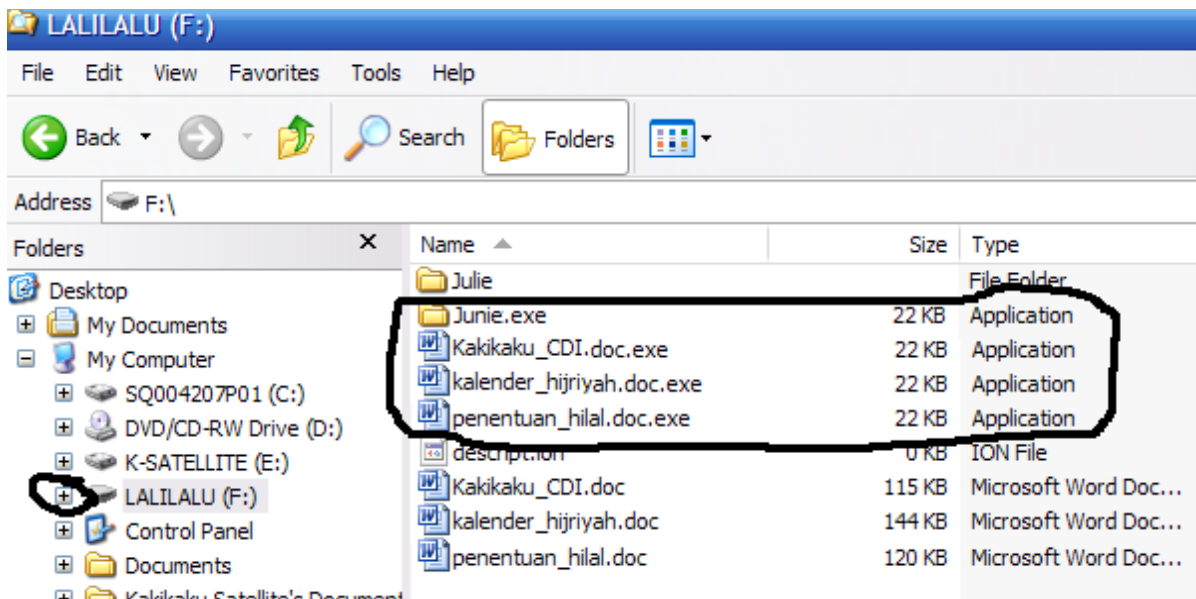
4. **File atau icon atau folder yang sepiantas familiar dan aman padahal belum tentu aman**
Mungkin banyak pembaca yang sudah menyadari bahwa contoh pada tips sebelumnya itu mudah dikenali karena file-file aneh tersebut memiliki icon yang berbeda dan tidak familiar, tapi tidak semua malware itu “pemberani” yaitu dengan menampilkan icon yang sesungguhnya, karena ada sebagian malware “yang pengecut” dengan menyamar/menyerupai icon file yang familiar.

Sebagai contoh : Pemilik UFD Lalilalu membuka Windows Explorer (shortcut : tombol windows + E), isi UFD Lalilalu adalah sebagai berikut :



Gambar L.5

UFD Lalilalu itu berisi 3 file **kakikaku_CDI.doc**, **kalender_hijriyah.doc**, dan **penentuan hilal.doc**, dan 2 folder : **Junie** dan **Julie**. Lalu UFD Lalilalu itu dipakai lagi untuk transfer data di komputer lain, terutama rental dan warnet. Ketika UFD Lalilalu kembali dimasukkan ke komputer pemilik UFD Lalilalu, ternyata ada beberapa file aneh seperti pada gambar di bawah ini :



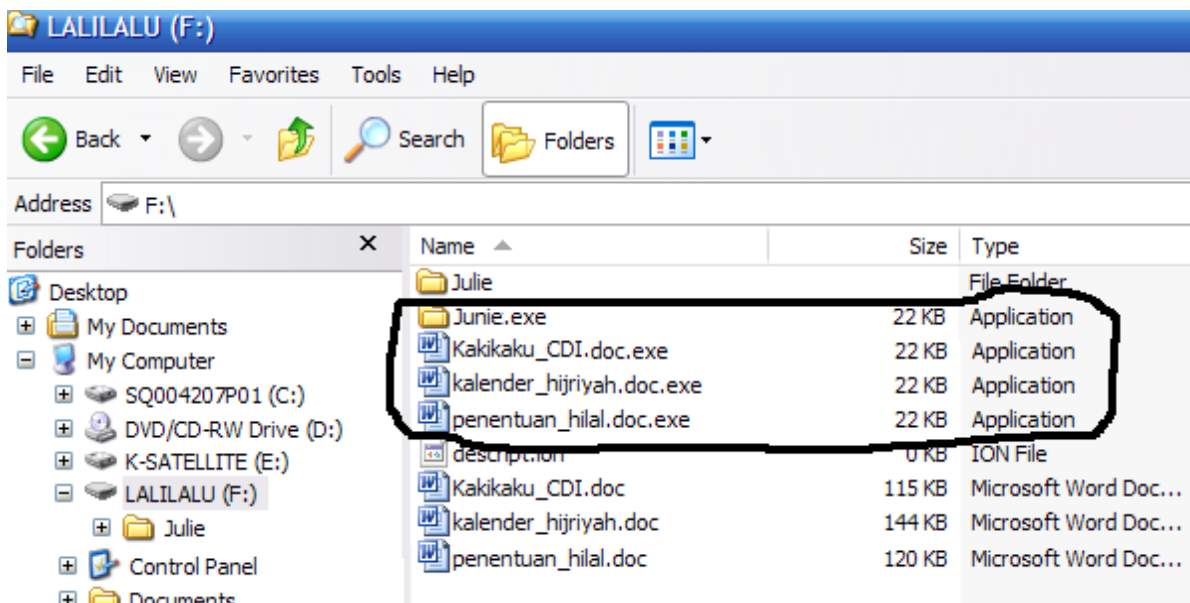
Gambar L.6

File-file yang mencurigakan kali ini adalah : folder **Junie(.exe)**, dan file **kakikaku_CDI.doc.exe**, **kalender_hijriyah.doc.exe**, dan **penentuan hilal.doc.exe**. Alasannya adalah :

- Sekalipun icon berbentuk Word, tetapi extention file-nya adalah .exe (jika tidak hati-hati Anda bisa saja salah membuka file, oleh karena itu pada View pada Windows Explorer-nya adalah Detail [Klik kanan pada area kosong Windows Explorer-->View-->Detail : Lihat gambar L.5]).

- Type pada folder **Junie**, dan file **kakikaku_CDI.doc.exe**, **kalender_hijriyah.doc.exe**, dan **penentuan hilal.doc.exe** adalah **Application**, padahal seharusnya Type **Junie** adalah **File Folder**, dan Type tiga file lainnya adalah **Word**, serta file-nya memang hanya ada 3 dan bukan 6.
- Size pada folder **Junie**, dan file **kakikaku_CDI.doc.exe**, **kalender_hijriyah.doc.exe**, dan **penentuan hilal.doc.exe** adalah sama, yaitu **22 KB**, padahal 3 file dokumen yang asli yang berbeda pasti berbeda size-nya, tapi file tersebut ternyata memiliki size yang sama.

Mungkin akan ada yang penasaran dengan folder **Junie** itu, dan mungkin akan ada yang berpendapat bahwa itu bukanlah malware. Untuk membuktikannya secara mudah adalah dengan meng-click tanda panah pada Lalilalu (F:), jika memang **Junie** itu adalah folder, maka ia akan folder tree-nya akan muncul setelah tanda panah pada Lalilalu (F:) telah diclick.



Gambar L.7

Setelah click, ternyata folder tree yang tampak hanyalah folder **Julie**, ini bukti bahwa **Junie** itu memang bukan folder, melainkan sudah menjadi file(.exe) yang mencurigakan. Oleh karena itu file folder **Junie**, dan file **kakikaku_CDI.doc.exe**, **kalender_hijriyah.doc.exe**, dan **penentuan hilal.doc.exe** hanya perlu dihapus.

5. Tetap waspada!!

Point 5 ini adalah sebagai pelengkap dari poin-poin sebelumnya :

- Terkadang ekstensi file tidak terlihat karena show hidden files tidak diaktifkan atau sistem komputer Anda sudah terinfeksi malware. Maka patokannya bukan hanya dari file extension (.exe, .doc, .docx), tapi bisa juga dari **size** dan **type**. Icon tidak bisa dijadikan patokan karena cukup banyak malware yang menyamar dengan icon yang familiar.
- Seringkali file yang asli disembunyikan oleh malware, sedangkan yang tampak adalah file yang palsu, maka selalu waspada dan berpatokan dengan extension, size, dan type.
- File asli yang disembunyikan oleh malware masih bisa diselamatkan dan ditampilkan kembali dengan menggunakan software lain seperti DOS atau software lain yang lebih mudah lagi, contohnya adalah ACD SEE (belilah ACD SEE original jika ingin selalu

- menggunakan software ini).
- File asli yang terhapus oleh malware masih ada kemungkinan untuk diselamatkan dengan menggunakan software data recovery.
 - Intinya adalah kewaspadaan. Pertama, biasakanlah dan terus memerhatikan situasi dan kondisi komputer atau data Anda, lalu jika mendapatkan suatu hal yang tidak biasa pada komputer atau data Anda, maka waspadalah terhadap hal aneh itu, lalu temukan solusinya (dengan mencari penyebabnya dan memastikan hal aneh itu), lalu terapkanlah solusi itu!

Demikianlah beberapa tips penulis agar dapat menghindari malware, semoga tips ini bermanfaat untuk kita semua. Amin. Tetap waspada!

Yusuf KS (merindukan waktu luang yang panjang)

Weblog : <http://myks.wordpress.com>

Link this article : <http://myks.wordpress.com/2008/07/13/tips-menghindari-malware>

PDF Version : http://www.kakikaku.com/yks/articles/tips_menghindari_malware.pdf

* Jika sistem komputer Anda ingin lebih kebal terhadap malware dan ingin jarang mendapat bahaya malware, maka gunakanlah sistem operasi Linux. Secara umum Linux lebih aman daripada Windows dan hampir semua distro Linux (dan software-software-nya) itu gratis. Gunakanlah Windows original jika Anda ingin menggunakan Windows, tapi jangan lupa untuk selalu waspada terhadap bahaya malware.