Belajar Tipu Muslihat Virus dan Pencegahannya

Fandi Gunawan
fandigunawan@gmail.com
http://fandigunawan.wordpress.com

Beberapa saat yang lalu penulis bertemu dengan seorang teman yang sedang mengalami masalah yaitu laporan tugasnya terinfeksi virus. Penulis melihat bahwa anti-virus yang dipakai teman saya cukup up-to-date namun ia tidak dapat mendeteksi virus tersebut. Setelah beberapa lama teman saya bercerita bahwa ia termakan tipu muslihat virus : dokumennya berikon ala dokumen Word. Selain cerita diatas penulis secara pribadi sering menjumpai masalah serupa dimilis-milis. Berikut penulis akan memaparkan sedikit tips untuk beberapa mencegah kita termakan muslihat virus baru yang belum terdeteksi anti-virus.

Sebelum menginjak kedalam tips mengenai pencegahan kita termakan muslihat virus ada baiknya kita pelajari sesuatu yang dikenal dengan nama teknik rekayasa sosial atau *Social Engineering* dalam bahasa Inggrisnya.

Teknik rekayasa sosial menurut RFC 2828 (Internet Security Glossary) dapat diartikan :
Jargon halus untuk kemampuan non-teknis atau rendah teknologi seperti tipuan, trik, ancaman yang digunakan untuk menyerang sistem informasi.

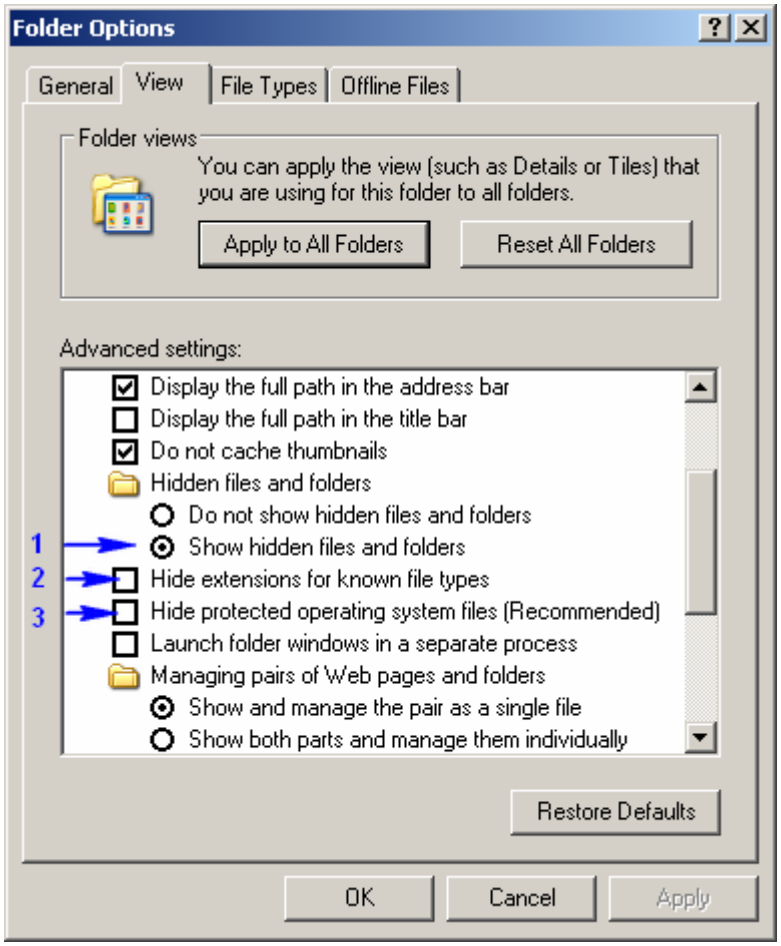
Mayoritas dari pengguna Windows terinfeksi virus disebabkan oleh karena adanya teknik rekayasa sosial ini. Hal inilah yang membuat virus cepat menyebar. Kekurangpahaman kita menjadikan hal ini menjadi senjata yang cukup mematikan dalam penyebaran dan penginfeksian virus.

Beberapa contoh yang sering saya jumpai yaitu :

1. Email palsu berlampirkan virus dengan judul yang ”menarik perhatian”
2. Virus dengan ikon yang sangat kita kenal semisal :
    a. Ikon dokumen Microsoft Office
    b. Ikon folder
    c. Ikon gambar, video dll
    d. Ikon *installer*
3. Sistem *auto-run* yang disalahgunakan untuk penyebaran virus

Berikut tips umum yang akan membantu Anda untuk mencegah kita termakan muslihat virus.

1. Selalu nyalakan opsi berikut di *folder options*:



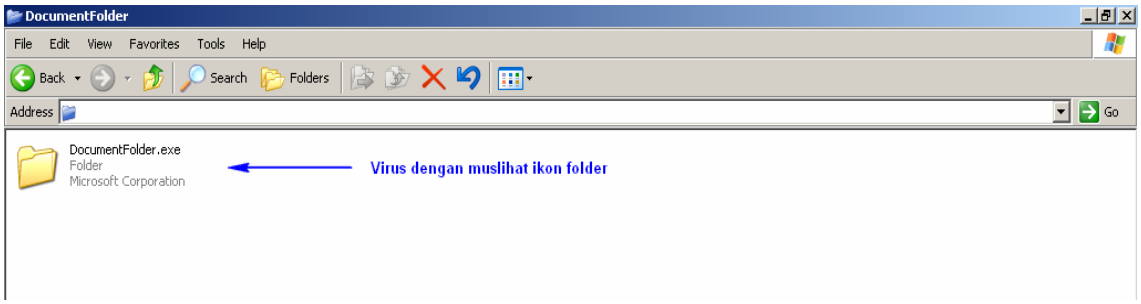
Catatan :
Opsi 1 digunakan untuk menampilkan folder dan berkas yang beratribut *hidden*.
Opsi 2 digunakan untuk menampilkan ekstensi berkas-berkas yang ada di Windows semisal berkas Microsoft Word adalah berekstensi .doc atau .docx.
Opsi 3 digunakan untuk menampilkan folder atau file yang beratribut *system*.
Opsi-opsi yang ada di folder options ini dapat juga *dikerjai* oleh virus sehingga kita tidak dapat mengubah opsi-opsi ini. Untuk sistem yang pernah *dikerjai* oleh virus sehingga kita tidak dapat mengubah opsi di folder options ini, penulis menyarankan penggunaan The Killer Machine atau antivirus dari vb-bego.com untuk mengembalikan pengaturan seperti sedia kala.

2. Ganti ikon standar Windows dengan beberapa alat gratis/berbayar yang ada di internet. Beberapa alat yang dapat dipakai :
   a. ActivIcons (http://www.cursorarts.com)
   b. IconPackager (http://www.stardock.com)

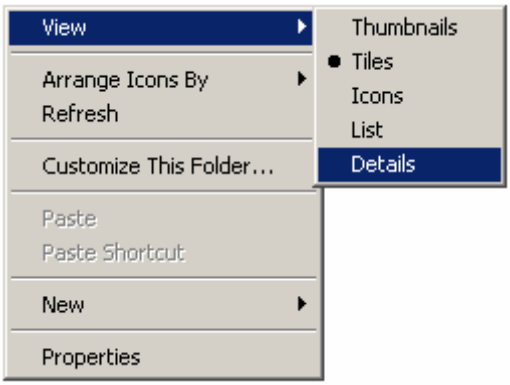
   Berikut contoh yang penulis pakai dengan mengganti warna asli folder sehingga

   bila ada virus yang mengelabui :

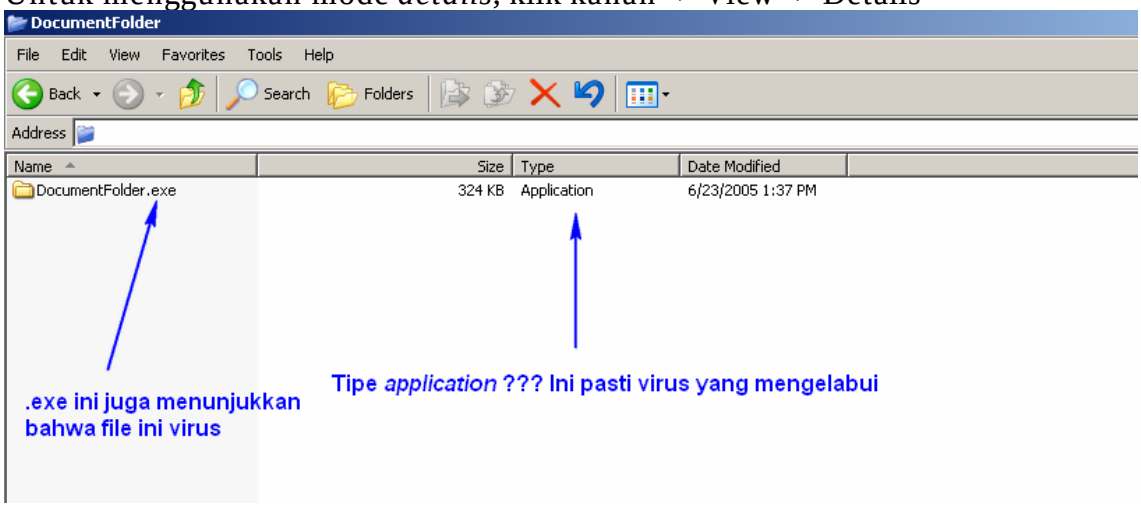
3. Gunakan mode *details* untuk menampilkan berkas-berkas dan folder



Menggunakan mode *tiles*, namun terlihat juga berbentuk .exe karena penulis menggunakan opsi 2 di *folder options* untuk menampilkan ekstensi berkas-berkas yang ada di Windows.



Untuk menggunakan mode *details*, klik kanan -> View -> Details

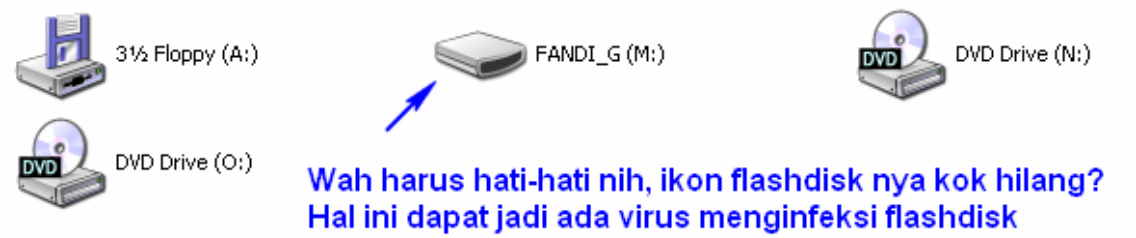


4. Untuk flashdisk atau harddisk gunakan ikon untuk tanda terkena virus atau tidak, berikut contohnya:

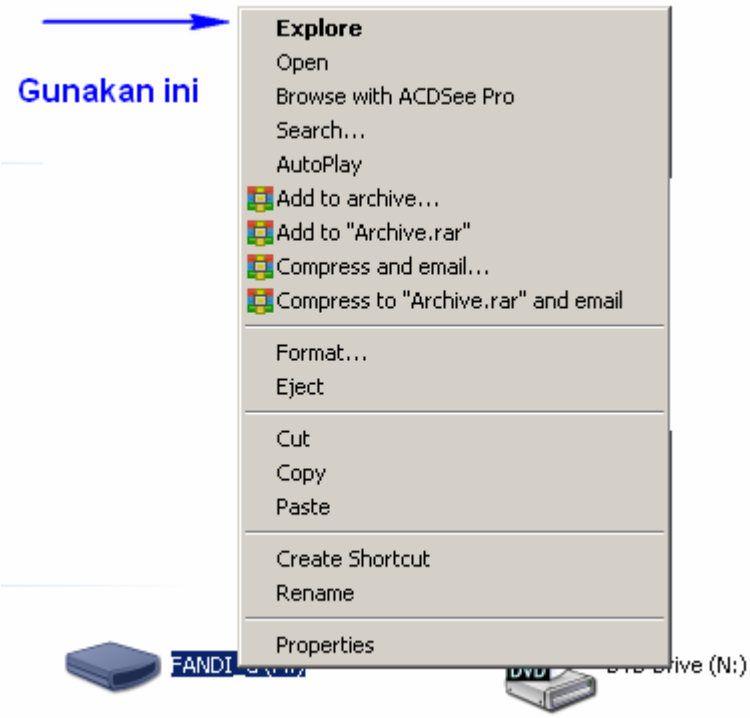
Untuk membuatnya cukup mudah. Buka notepad kopikan kode berikut dan *save-as* autorun.inf

[autorun]
icon=nama_icon.ico

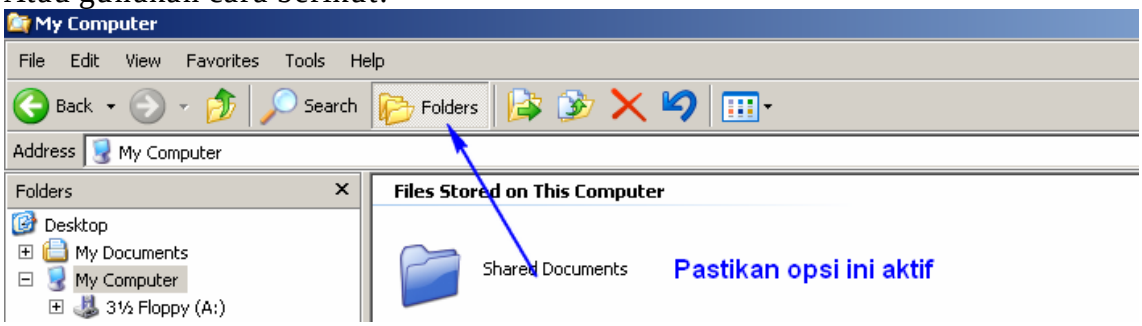
Apabila ada infeksi virus kita akan segera mengetahuinya!
Berikut contoh ketika flashdisk terinfeksi virus.



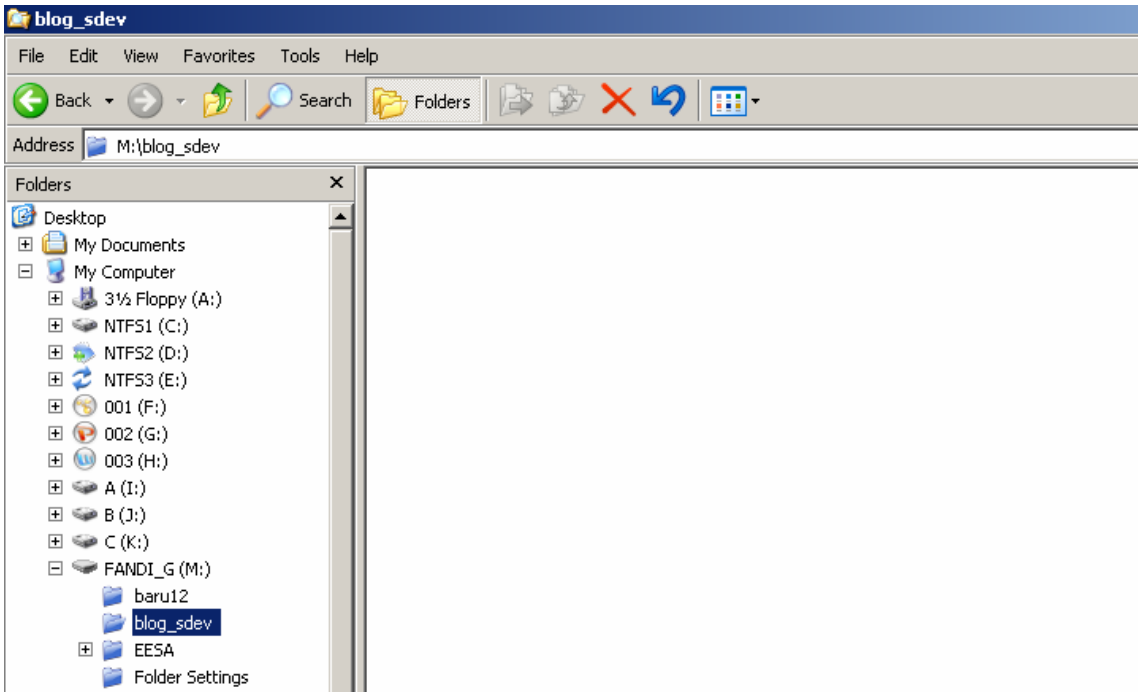
5. Untuk flashdisk atau harddisk jangan pernah gunakan klik ganda untuk membuka *root* direktorinya. Sebaiknya gunakan *explore*



Atau gunakan cara berikut:



Untuk meng-*explore* kita gunakan *tree-view* sebelah kiri.

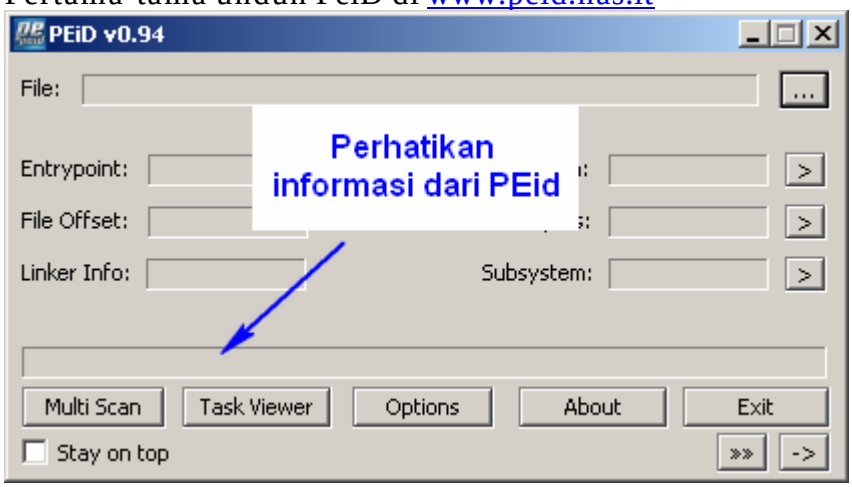


6. Ketika menancapkan flashdisk ke port USB tahan *shift* untuk mematikan fitur *auto-run*

Tips khusus untuk mengidentifikasi virus

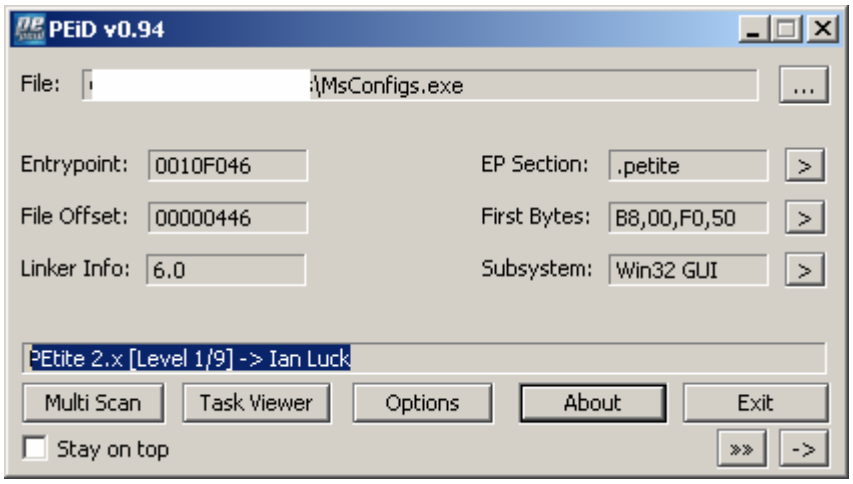
1. Installer palsu (berbentuk .exe)

Pertama-tama unduh PeiD di www.peid.has.it

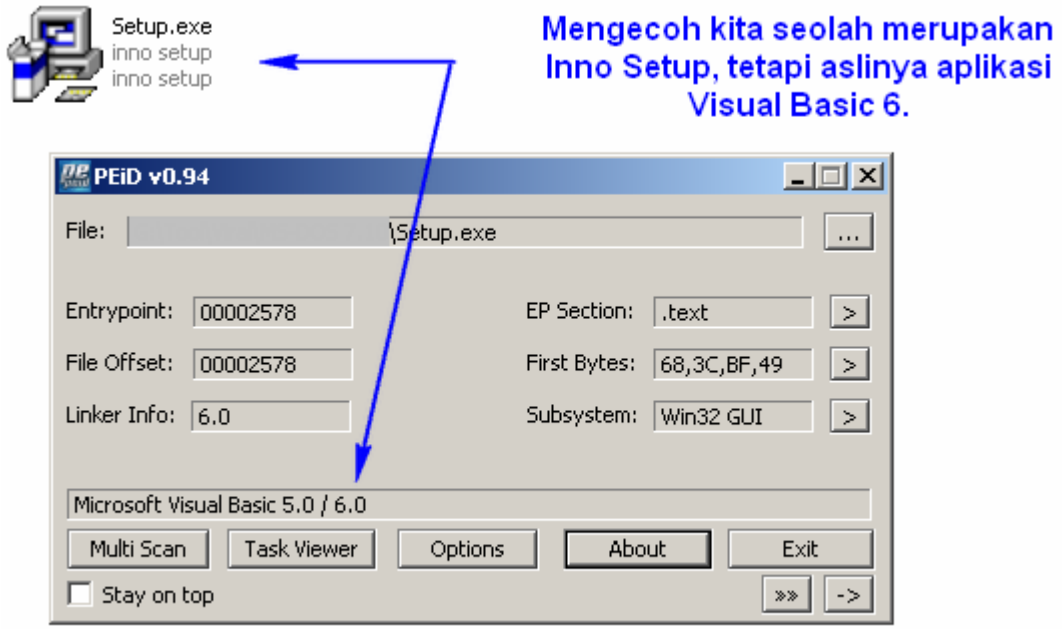


PEiD merupakan sebuah alat untuk mengidentifikasi sebuah file .exe berformat PE.

Mari kita lihat di PEiD



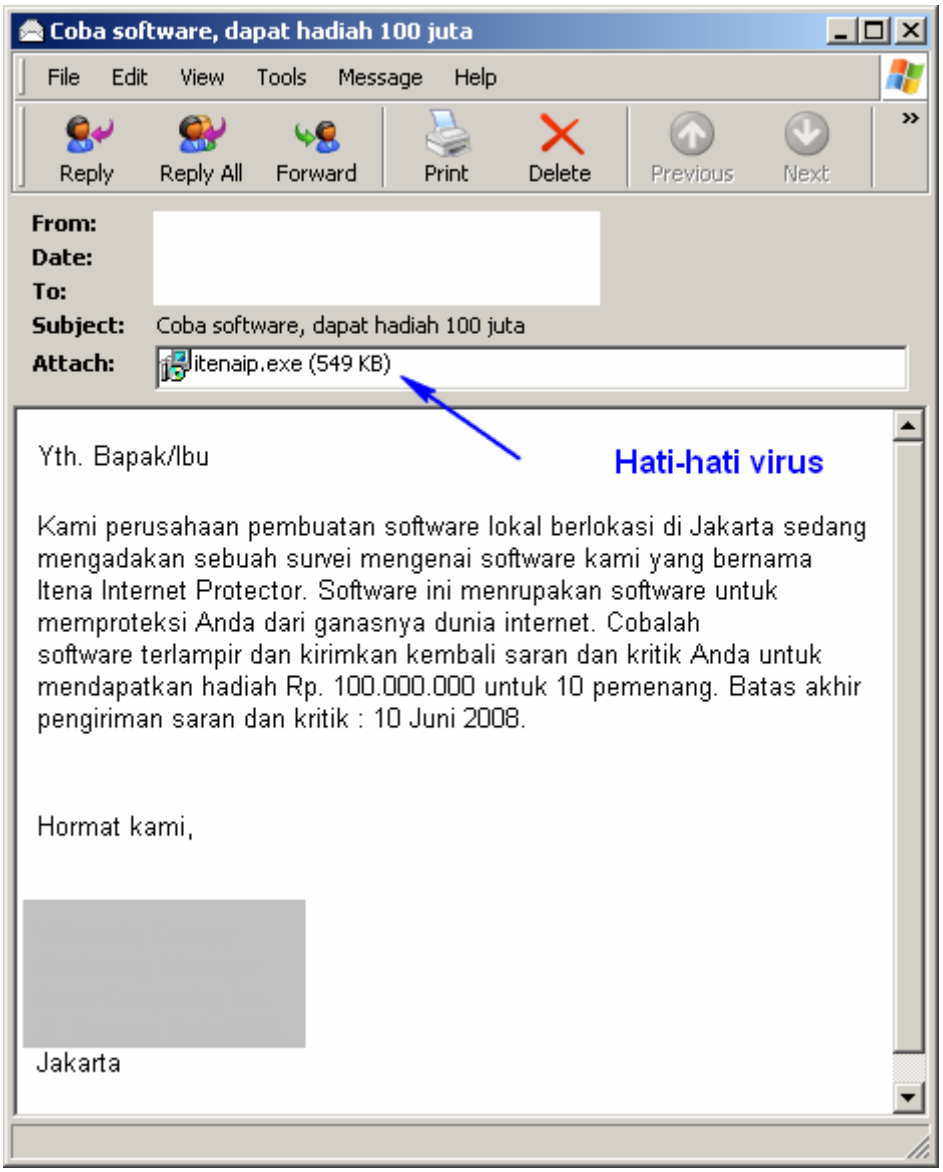
Ternyata file tersebut merupakan .exe yang dipaket dengan **petite**. Sebagai informasi saja saya jarang sekali melihat installer dipaket dengan **petite**. Berikut contoh lainnya :



Installer pada umumnya dibuat dengan :

- ✓ RAR SFX (RAR self extractor)
- ✓ WinZIP SFX (WinZIP self extractor)
- ✓ Installshield
- ✓ Inno Setup
- ✓ Nullsoft Scriptable Install System (Nullsoft PiMP SFX)
- ✓ Wise Installer
- ✓ Windows SFX installer
- ✓ GP-Install

2. Email dengan lampiran mencurigakan



Jangan membuka e-mail dari orang lain terutama yang berekstensi .exe, .zip, .rar kecuali Anda sudah mendapatkan konfirmasi mengenai pengiriman. Jangan membuka e-mail dengan judul yang "menggiurkan" semisal tentang lotere, pornografi, hadiah gratis dan lain-lain.

Kesimpulan:

Berhati-hatilah karena teknik rekayasa sosial menggunakan tipu muslihat untuk menyebarkan virus dan menginfeksikan virus. Teknik rekayasa sosial ini diperoleh dari kebiasaan kita menggunakan sesuatu yang digunakan sebagai senjata. Waspadalah-waspadalah! (kata Bang Napi)

BIOGRAFI PENULIS

Fandi Gunawan. Menamatkan SMU di SMUN 2 Kediri tahun 2004. Kini sedang menyelesaikan kuliah S1 Electrical Engineering di President University. Sekarang sedang aktif dalam membangun komunitas berbasis opensource. Gemar mempelajari tentang celah keamanan, *reverse engineering*, antarmuka piranti keras, pemrograman piranti keras, desain prosesor (SPARC, 8051, PIC, MIPS dan ARM), desain OS dan kriptografi piranti keras. Bahasa pemrograman yang pernah dipakai : Pascal, bahasa rakitan MIPS, bahasa rakitan 8051, C untuk 8051, C untuk AVR, C untuk PIC dan C untuk komputer, C#, VHDL dan Java. Berkecimpung dalam dunia OS yang melingkupi :
FreeDOS, MSDOS, Linux (pelbagai distro), FreeBSD, OpenBSD, NetBSD dan Windows (pelbagai versi).

URL : http://fandigunawan.wordpress.com (blog)
URL : http://kaktusaja.co.cc (Kaktus Aja!)
URL : http://eepu.wordpress.com (EESA of PU)
URL : http://coredotnet.co.cc (Core.NET of PU)

E-Mail : fandigunawan@gmail.com