

Virus Manfaatkan Autostart Windows

Anharku

v_maker@yahoo.com

http://anharku.freevar.com

Lisensi Dokumen:

Copyright © 2003-2009 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.

Bagi yang udah master jangan baca artikel ini kalau hanya akan merasa membuang2 waktu saja. Artikel ini di buat untuk membuka pengetahuan kita tentang autostart virus, bagaimana virus tersebut bisa memulai aktivitasnya aktivitas mempertahankan diri dari ancaman Av, aktivitas penyebaran (beranak-pinak), dan aktivitas-aktivitas lainnya (terserah VM-nya). Nah bagaimana virus tersebut bisa aktif (mengaktifkan diri) setiap kamu mulai menyalakan computer kamu? Jawabannya adalah virus tersebut memanfaatkan metode autostart pada windows. Lalu metode-metode autostart window itu apa aja?

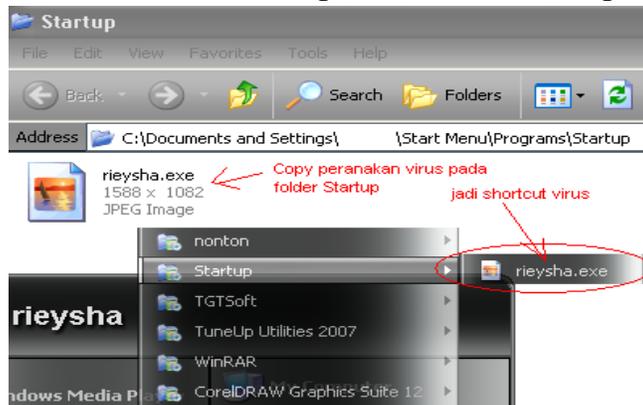
1. Memanipulasi Registry

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsCurrent\Version dengan key :

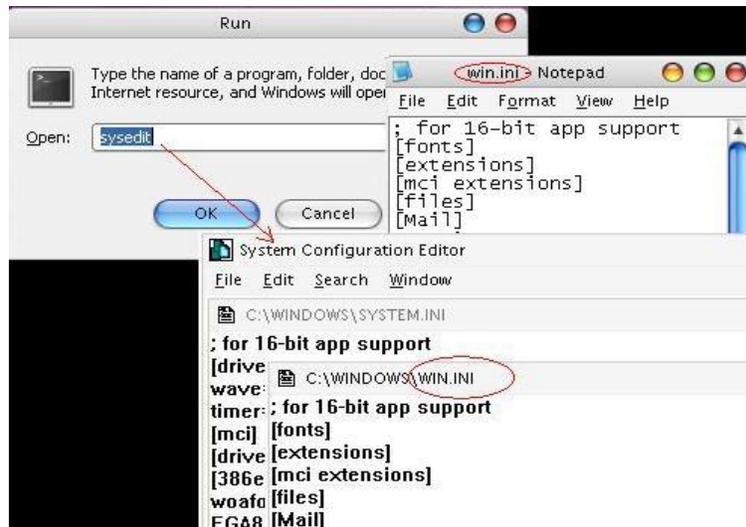
- Run
- RunOne
- RunOnceEx
- RunService
- RunServiceOnce

Manipulasi registry Juga dilakukan pada HKEY_CURRENT_USER-nya.

2. Menduplikasi (membuat peranakan virus) atau membuat shortcut pada directori C:\Documents and Settings\xxx\Start Menu\Programs\Startup



3. Memanipulasi win.ini



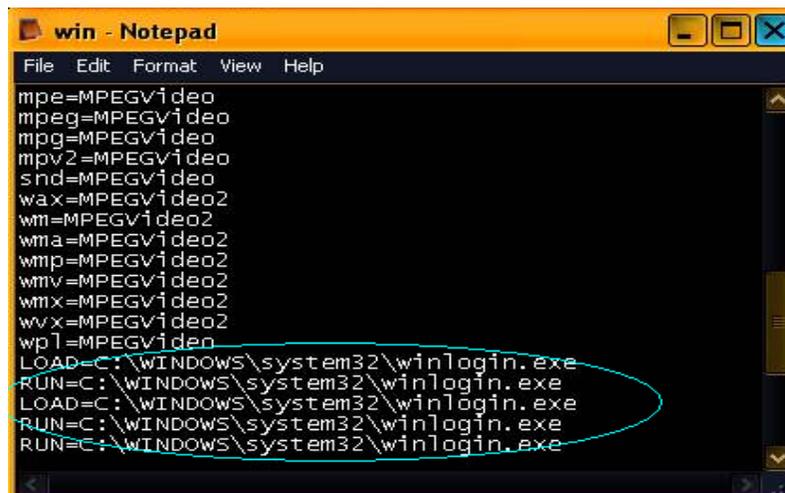
System Editor atau disingkat Sysedit adalah file bawaan windows yang dijalankan ketika computer masuk ke windows perama kali, seperti halnya regedit. Jadi manipulasi terhadap file win.ini pada sysedit tersebut dapat digunakan sebagai start-up bagi virus (baca:start-up tersembunyi). Loh kok tersembunyi? Karena biasanya user tidak sadar jika file win.ini tersebut telah dimanipulasi oleh virus. Manipulasi win.ini dilakukan dengan Menggunakan perintah LOAD= atau RUN= dan menambahkan pada baris:

[Windows]

load=C:\lokasiVIRUS\nama VIRUS.exe

run=C:\lokasiVIRUS\nama VIRUS.exe

NAH seperti ini contoh file win.ini yang udah dimanipulasi oleh virus **W32/VB Worm.MLG**



Karena file win.ini juga merupakan file yang dieksekusi pertama oleh windows, file ini berisi aplikasi 16 bit yang di-support oleh windows.



4. Memanipulasi autoexec.bat

secara win nama Virus, dimana nama Virus adalah Virus yang diaktifkan. Virus tersebut akan dijalankan dari mode Dos.

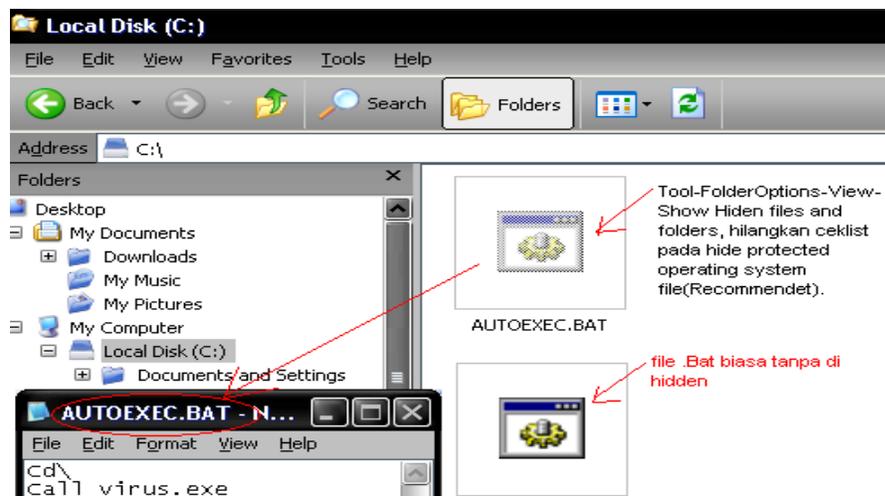
Manipulasi autoexec.bat dilakukan dengan Menggunakan perintah **Call** dan menambahkan pada baris

Call virus.exe

Misal virus peranakan virus terdapat di C:\ maka tulis

Cd\
C:\

Call virus.exe



Sama seperti saat kamu memanggil aplikasi menggunakan Command Prompt masuk dahulu ke folder yang dituju lalu ketik nama plikasi tersebut, maka aplikasi tersebut akan dijalankan.

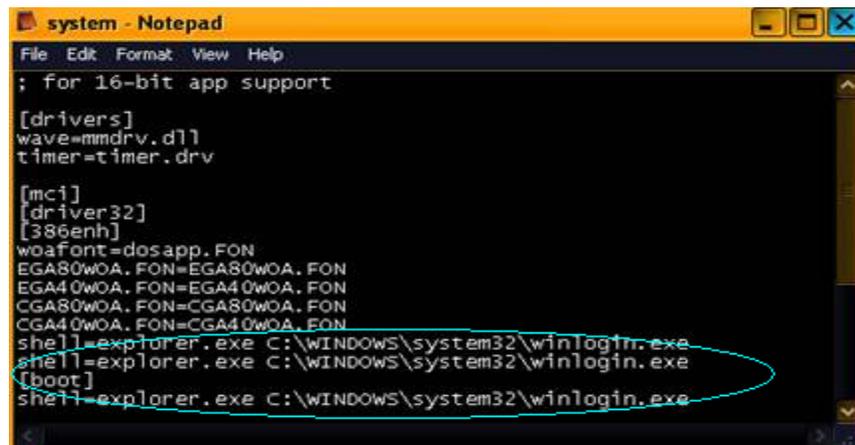
5. Memanipulasi system.ini

Manipulasi system.ini dilakukan dengan Menggunakan perintah Shell= dan menambahkan pada baris

[boot]

shell=explorer.exe C:\lokasiVIRUS\namaVIRUS.exe

NAH seperti ini contoh file system.ini yang udah dimanipulasi oleh virus W32/VBWorm.MLG



```
system - Notepad
File Edit Format View Help
; for 16-bit app support

[drivers]
wave=mmdrv.dll
timer=timer.driv

[mci]
[driver32]
[386enh]
woaFont=dosapp.FON
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON
shell=explorer.exe C:\WINDOWS\system32\winlogin.exe
shell=explorer.exe C:\WINDOWS\system32\winlogin.exe
[boot]
shell=explorer.exe C:\WINDOWS\system32\winlogin.exe
```

Nah2..udah tau kan autostart dari komputermu sendiri? Sekarang seting-seting aja apa yang akan dijalankan pertama saat komputermu dinyalakan (diStart-up)© Cara setingnya dah tahukan? Gunakan System Configuration Utility,caranya ketik msconfig pada kotak dialog Run-OK. Untuk mendisable program, pilih tab General, klik Selective Startup lalu hilangkan tanda ceklist pada Process WIN.INI dan Load Startup Items. Atau, untuk mendisable item tertentu, pilih tab Startup atau WIN.INI, lalu hilangkan tanda ceklist pada item yang ingin kamu disable. Kamu juga bisa mengklik Disable All pada tab Startup dan WIN.INI untuk men-disable semua item pada masing-masing tab. Kamu juga bisa memaksimalkan kerja computer kamu dengan menseting services yang akan dijalankan,hilangkan ceklist pada service yang tidak dibutuhkan-tekan OK lalu restart untuk melihat perubahannya.Semoga apa yang saya tuliskan dapat membuka pengetahuan anda.

Biografi Penulis



Anharku. Pertama mengenal komputer saat SMP pertamanya kenal komputer hanya bermain game bawaan window's lambat laun karna pergaulan dan pertumbuhan,merasakan anehnya cinta monyet...patahhati lalu melampiaskannya pada bermain Game online namun karena satu persatu game itu servernya runtuh (gameOver kali) jadi aku memutuskan vakum dari dunia gamer waktu itu juga saat aku masih UAS jadi aku fokus ke skull dulu.Lanjut mengenal dunia internet sejak hobi main di warnet untuk sekedarmengecek e-mail, fs, dan

sekedar chatting ga jelas..Dari temanku bernama DNZ lah aku mulai mengenal dunia virus..lalu aku belajar secara otodidak karna temanku DNZ lebih suka dunia Hacking. Belajar algoritma dan pemrograman, membuat flowchart,dan belajar bahasa pemrogramanseperti visual basic, delphi, C++, pascal, asmbly. Belajar tentang micro, website, PHP, Basis data, MySQL,belajar tentang Jaringan Komputer..belajar tentang segala sesuatu yang berbau komputer.