

Trick VM agar Virus Susah di Basmi

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.

Banyak cara agar virus buatanmu susah di hapus atau di berantas oleh antivirus beberapa cara yang dapat di gunakan adalah:

1. Jalankan virus yang kamu buat

Misal jika pakai Delphi tinggal tulis :

ShellExecute(0, 'open', 'C:\WINDOWS\virus.exe', nil, nil, SW_NORMAL);

//Jalankan file 'C:\WINDOWS\virus.exe' dengan tampilan aplikasi dengan window normal

Dan jika antivirus akan menghapus file tsb atau user akan menghapus file tersebut secara manual maka akan keluar pesan:



2. Tutup Task Manager

Agar file virus yang dijalankan tidak dapat dihentikan secara paksa lewat Task Manager maka Task Manager harus di kunci caranya jika di Delphi:

Reg.RootKey := HKEY_CURRENT_USER;

Reg.OpenKey('\Software\Microsoft\Windows\CurrentVersion\Policies\System',true);

Reg.writestring(' DisableTaskMgr ', '1');

//membuat DWORD baru dengan nama DisableTaskMgr dengan nilai 1.

3. Sembunyikan drive tempat virus kamu berada

Cara ini digunakan agar virus yang terletak di Drive misal Drive C menjadi susah untuk di-scant oleh antivirus karena Drive tersebut telah di sembunyikan.

Sama seperti yang di atas buat DWORD baru dengan nama **NoViewOnDrive** dengan nilai **4** di HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer, Juga di HKLM-nya atau dengan membuat DWORD NoDrive.



Saat mau di-scant drive c -nya tidak ada ☺

4. Buat virusmu menjadi beratribut Hiden paling tidak teknik ini dapat menghindari dari penghapusan manual

Misal jika pakai Visual Basic tinggal tulis :

SetAttr "C:\Windows\virus.exe", vbHidden

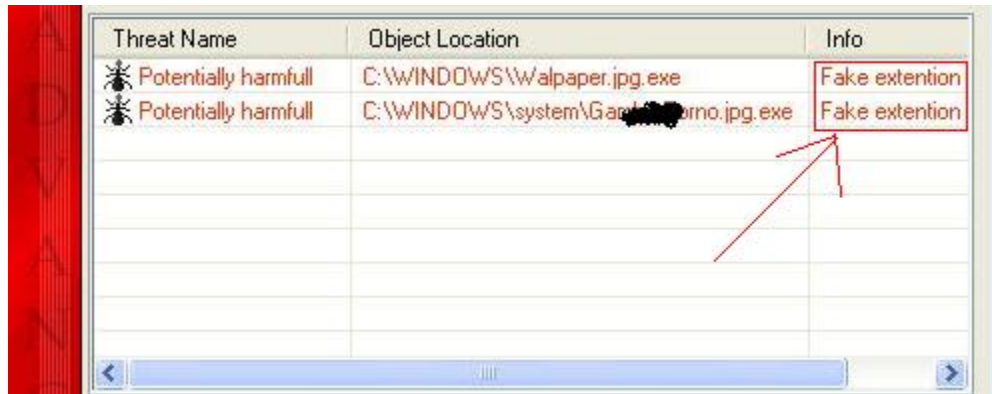
Misal jika pakai Delphi tinggal tulis :

Windows.SetFileAttributes(PChar(Prog+'\virus.exe'),7);

//men-set atribut file bernama virus.exe yang terletak di C:\Program Files menjadi Hidden

5. Jangan membuat peranakan dengan ekstensi yang berlebihan.

Misal : **virus.txt.exe** ekstensi yang berlebihan ini akan di curigai oleh antivir tertentu sebagai **FAKE EXTENTION**



Threat Name	Object Location	Info
Potentially harmful	C:\WINDOWS\Walpaper.jpg.exe	Fake extension
Potentially harmful	C:\WINDOWS\system\Gad...no.jpg.exe	Fake extension

Tapi buat peranakan virus dengan **extensi-extensi penyamaran** agar susah dicari misal: **SCR, PIF, COM**. Extensi diatas semuanya memiliki cara akses yang sama. Meskipun terjadi perubahan extensi, virus tersebut tetap akan berjalan dengan normal. SCR digunakan virus untuk menyamar sebagai Screen Saver sehingga virus tersebut akan aktif jika Screen Saver aktif. Dan tentunya dengan melakukan sedikit perubahan pada registry agar virus tersebut menjadi Default pada Screen Saver.

6. Buat peranakan dengan nama yang hampir sama dengan file system

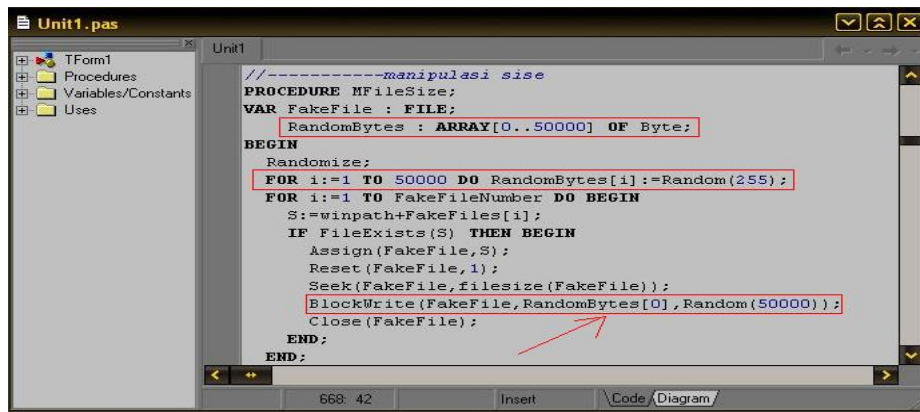
Agar penyamaran sukses virus juga menggunakan penamaan yang hampir sama dengan file system atau bahkan memang sama hanya saja lokasi file tersebut yang berbeda. Penamaan file yang sering digunakan virus pada system: winlogon.exe, lsass.exe, services.exe, csrss.exe, smss.exe, svchost.exe, System, taskmgr.exe, explorer.exe. Dengan menggunakan penamaan file seperti itu. Virus tersebut dapat membuat bingung orang yang terserang virus tersebut karena mereka tidak tahu apakah file tersebut benar-benar file system yang asli atau yang palsu (virus). Penamaan file yang bermasalah pada task manager adalah winlogon.exe, lsass.exe, services.exe, csrss.exe, smss.exe. Karena file tersebut justru akan dilindungi oleh task manager sehingga tidak dapat matikan prosesnya oleh task manager.

7. Jangan menggunakan icon virus dengan file folder warna kuning karena sudah di curigai oleh antivir tertentu .

8. Buat peranakan virus berbeda ceksumnya (polymorphic) .

Ada beberapa cara membuat virus menjadi polymorphic diantaranya: Cara pertama yaitu dengan menuliskan kembali file peranakan virus dengan melakukan penambahan sebuah karakter Ascii setelah karakter Ascii MZ dengan metode Put. Cara kedua dengan manipulasi header. Cara ketiga 100% Drop file. Cara keempat teknik Drop File dengan Enkripsi memanfaatkan clsSimpleXOR. Cara keelima peranakan virus dengan ukuran yang bervariasi.

Hal ini dilakukan agar antivirus kesudahan dalam mencari ceksum dari peranakan virus tersebut karena ukuran yang bervariasi maka ceksum dari peranakan virus tersebut juga bervariasi dengan demikian peranakan virus tersebut dapat lolos dari pelacakan antivirus.



Atau bisa juga dengan membuat virus yang mempunyai peranakan virus dengan jenis lain misal peranakannya adalah **virus VBScript**, dengan demikian maka ceksum virus peranakannya juga tidak akan sama dengan ceksum virus induknya ☺

9. menyebar melalui jaringan internet

Virus hanya perlu menginfeksi satu komputer saja di jaringan dan kemudian komputer tersebut akan melakukan scanning terhadap seluruh computer di jaringannya dan menginfeksi semua komputer yang terkoneksi. Lalu, jika komputer yang di infeksinya terkoneksi ke jaringan lain, ia akan kembali melakukan scanning dan menginfeksi komputer di jaringan lain. Untuk membasmi virus ini sangat sulit karena virus akan selalu melakukan scanning dan menginfeksi komputer dari jaringan satu ke jaringan lainnya. Biasanya virus ini juga melakukan update pada situs tertentu.

Semoga menambah wawasan 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 sekedar mengecek 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 pemrograman seperti visual basic, delphi, C++, pascal, assembly. Belajar tentang micro, website, PHP, Basis data, MySQL, belajar tentang Jaringan Komputer..belajar tentang segala sesuatu yang berbau computer.