Scan Virus by String

Anharku
v_maker@yahoo.com
http://anharku.freevar.com

Sebenarnya Mengapa sih bisa dikatakan suatu file adalah virus? Jawabanya yang paling umum pasti karna file tersebut mempunyai kemampuan untuk menggandakan diri,melakukan peng-Copy-an diri, Melakukan penyebaran agar virus memiliki keturunan yang akan melanjutkan perjuangan hidup meneruskan perjuangan induk virus yang sudah tua renta dan mati dibasmi oleh antivirus. Anak virus tersebut juga menggandakan diri (Seperti Induk) dan dalam penggandaan diri tersebut juga melakukan teknik penyebaran perjalanan dari computer satu ke computer lain. Lalu bagaimana suatu virus dapat melakukan pengandaan diri? Dalam Visual Basic perintah menggandakan dapat dilakukan dengan dua cara yaitu:

1. Menggunakan code standar dalam visual basic. (**FileCopy**).
2. menggunakan code API untuk yang akan berinteraksi langsung dengan system

1. Perintah Copy Visual Basic (FileCopy)
Dengan perintah perintah peng-copy-an suatu file pada visual basic, kita bisa membuat suatu fungsi untuk melakukan suatu penggandaan diri dalam suatu virus, tapi fungsi ini tidak 100% berhasil. Dan memakan waktu yang lama jika digunakan untuk melakukan penggandaan dalam jumlah banyak. Perintah ini sebaiknya digunakan jika kita ingin membuat suatu virus yang sederhana.
Code:

```
FileCopy sumber,tujuan
```

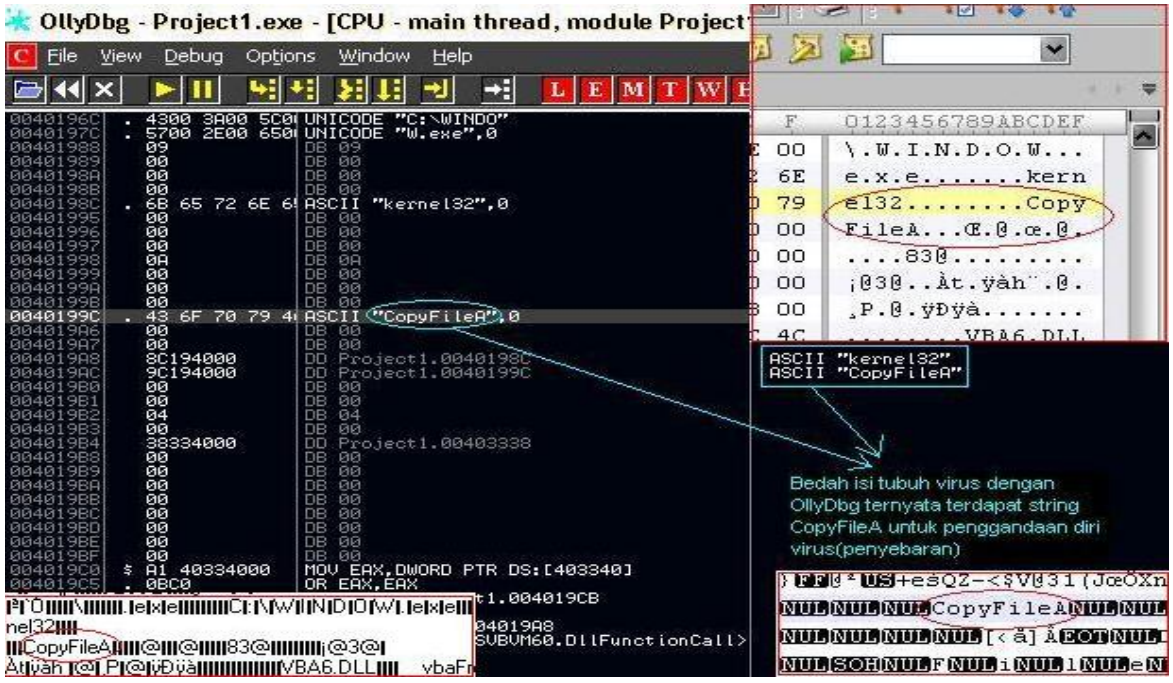
2. Fungsi API:
Penggunaan perintah API sangat disaran jika kita ingin membuat suatu applikasi yang professional. Kok Applikasi? Karena fungsi ini biasanya digunakan untuk membuat aplikasi installer yang dibuat oleh suatu perusahaan software. Fungsi API selalu digunakan oleh perusahaan software agar software yang mereka buat bisa langsung berinteraksi dengan system operasi dan bukan berinteraksi dengan sebuah file virtual machine (Contoh : msvbvm60.dll) dimana virtual machine ini berfungsi untuk melakukan hubungan dari suatu applikasi ke system operasi. Jadi baiknya jika aplikasi kita buat langsung berhubungan dengan system operasi sehingga kinerja dari aplikasi yang kita buat tersebut akan sangat baik. Apa hubungannya sama virus? Jika kita bisa membuat virus yang langsung berhubungan dengan system operasi. Selain proses penyebarannya sangat cepat, virus itupun mampu melindungi dirinya dengan sangat baik. Karena

ia mempu mengendalikan suatu aplikasi. Apakah aplikasi tersebut diperbolehkan untuk dijalankan atau tidak.

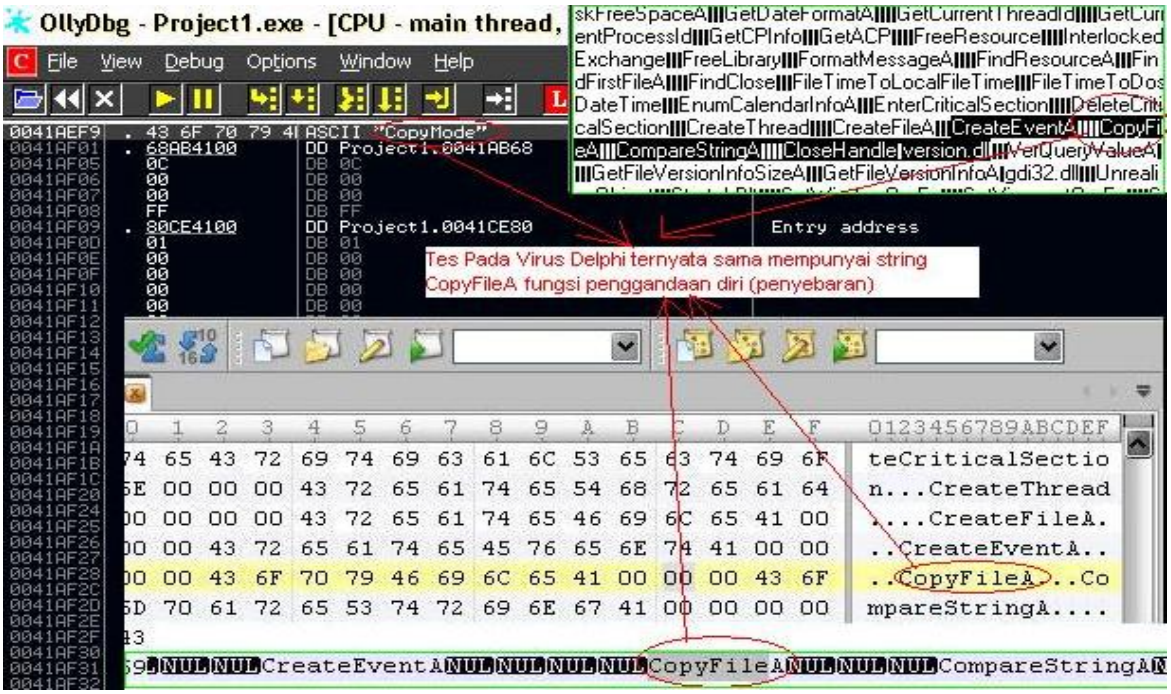
```
Public Declare Function CopyFile Lib "kernel32" Alias "CopyFileA" _
(ByVal lpExistingFileName As String, ByVal lpNewFileName As String, _
ByVal bFailIfExists As Long) As Long
```

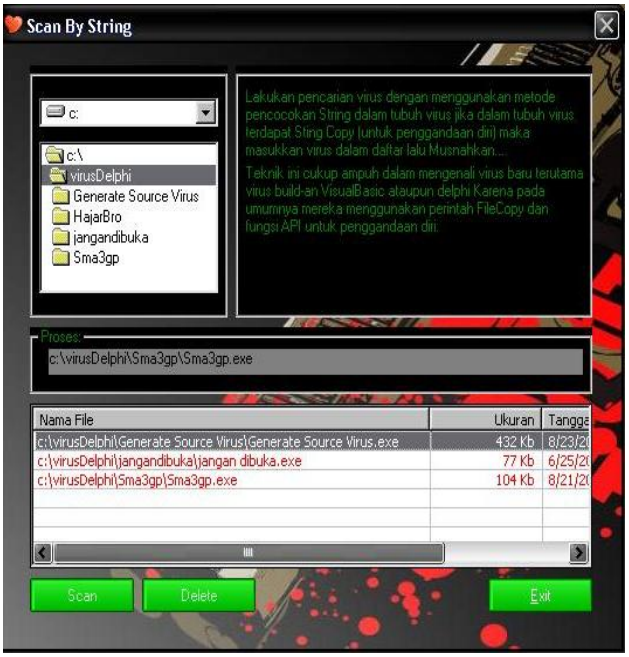
Lalu bagaimana jika di Delphi? Sama saja seperti pada Visual Basic yaitu dengan menggunakan code standar (**CopyFile**) dan menggunakan code API. Lalu bagaimana dengan bahasa-bahasa lainya? Bahasa C? Assembly?atau bahasa-bahasa lain yang digunakan dalam pembuatan virus?intinya sama String **Copy.**

Nah setelah mengetahui string apakah yang slalu ada dalam suatu file virus maka kita lakukan percobaan untuk melihat isi tubuh virus tersebut dengan tool-tool atau software-software penganalisa file executable. Kita coba bedah tubuh virus Visual Basic yang melakukan teknik pengcopy-an diri.



Lalu kita juga coba bedah tubuh virus Delphi yang melakukan teknik pengcopy-an diri.





Lakukan pencarian virus dengan menggunakan metode pencocokan String dalam tubuh virus jika dalam tubuh virus terdapat Sting **Copy** (untuk penggandaan diri) maka masukkan virus dalam daftar lalu Musnahkan....Teknik ini cukup ampuh dalam mengenali virus baru terutama virus build-an VisualBasic ataupun delphi Karena pada umumnya mereka menggunakan perintah **FileCopy** dan fungsi API untuk penggandaan diri.Klik di ListView virus yang tertangkap lalu tekan delete.

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, asmbly. Belajar tentang micro, website, PHP, Basis data, MySQL, belajar tentang Jaringan Komputer..belajar tentang segala sesuatu yang berbau komputer.*