MALWARE ANALYSIS REPORT ON MELISSA MALWARE

PRESENTED BY

SAYAN KANTI MUKHERJEE MT20ACS532

Contents

Overview

In this document, I have taken a malware sample and through various means of Static and dynamic malware analysis techniques, I have tried to identify the malware family and come up with the name, which is Melissa Malware. I have tried to cover the entire malware analysis process in this document including the basic characteristics of Melissa Malware.

Introduction

The Melissa virus was a mass-mailing macro virus released on or around March 26, 1999. The naming of the malware was done by Smith for a stripper in Florida, started by taking over victims' Microsoft Word program disabling a number of safeguards in Word 97 or Word 2000. Then a macro has been used to hijack their Microsoft Outlook email system and send messages to the first 50 addresses in their mailing lists. Those messages, in turn, tempted recipients to open a virus-laden attachment by giving it such names as "sexxxy.jpg" or "naked wife" or by deceitfully asserting, "Here is the document you requested ... don't show anyone else ;-)."

Technical Details

Melissa works with Microsoft Word 97, Microsoft Word 2000, and Microsoft Outlook 97 or 98 email client. One doesn't need to have Microsoft Outlook to receive the virus in email, but it will not spread itself further without it.

Melissa will not work under Word 95 and will not spread further under Outlook Express.

Melissa can infect Windows 95, 98, NT and Macintosh users. If the infected machine does not have Outlook or internet access at all, the virus will continue to spread locally within the user's own documents.

Propagation of Malware

Melissa arrives in an attachment to an e-mail note with the subject line "Important Message from [the name of someone]," and body text that reads "Here is that document you asked for...don't show anyone else ;-)". The attachment is often named LIST.DOC. If the recipient clicks on or otherwise opens the attachment, the infecting file is read to computer storage. The file itself originated in an Internet alt.sex newsgroup and contains a list of passwords for various Web sites that require memberships. The file also contains a Visual Basic script that copies the virus-infected file into the normal.dot template file used by Word for custom settings and default macros. It also creates this entry in the Windows registry:

HKEY_CURRENT_USERSoftwareMicrosoftOffice"Melissa?"="...by Kwyjibo"

The virus then creates an Outlook object using the Visual Basic code, reads the first 50 names in each Outlook Global Address Book, and sends each the same e-mail note with virus attachment that caused this particular infection. The virus only works with Outlook, not Outlook Express.

The email looked like this:

- From: (name of infected user)
- Subject: Important Message From (name of infected user)
- To: (50 names from alias list)
- Body: Here is that document you asked for ... don't show anyone else ;-)
- Attachment: LIST.DOC

We must remember that Melissa can arrive in any document, not necessarily just in this LIST.DOC where it was spread initially.

Most of the recipients are likely to open a document attachment like this, as it usually comes from someone they know.

Infection by Malware

After sending itself out, the virus continues to infect other Word documents. Eventually, these files can end up being mailed to other users as well. This can be potentially disastrous, as a user might inadvertently send out confidential data to outsiders.

The virus activates if it is executed when the minutes of the hour match the day of the month; for example, 18:27 on the 27th day of a month. At this time the virus will insert the following payload of text into the current open document in Word:

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

This text, as well as the alias name of the author of the virus, "Kwyjibo", are all references to the popular cartoon TV series called "The Simpsons".

Impact

Email servers at more than 300 corporations and government agencies worldwide became overloaded, and some had to be shut down entirely, including at Microsoft. Approximately one million email accounts were disrupted, and Internet traffic in some locations slowed to a crawl.

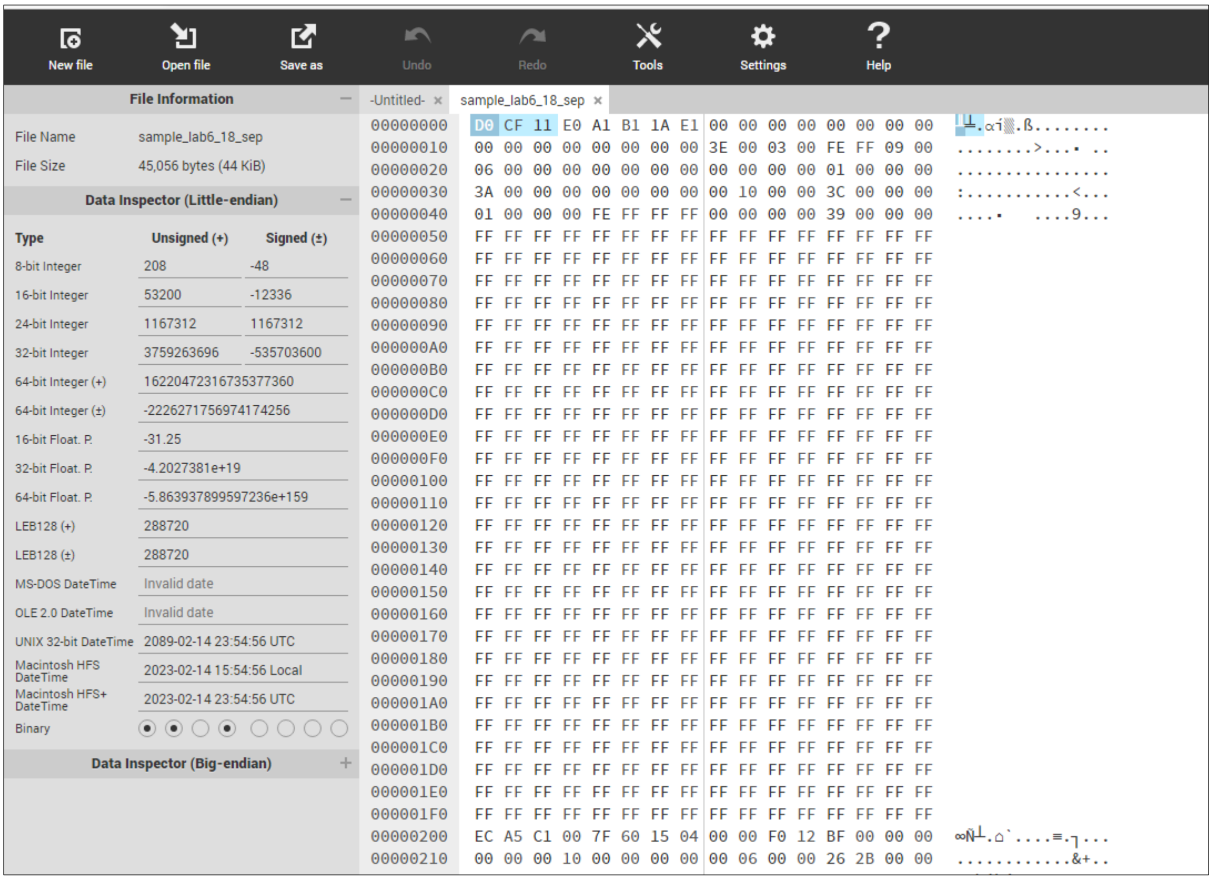
The collective damage was enormous: an estimated $80 million for the cleanup and repair of affected computer systems.

How to Avoid Melissa Malware attack

If we get an e-mail note with the subject, "Important Message from [the name of someone]," and it has an e-mail attachment (usually a 40-kilobyte document named LIST.DOC), simply DO NOT OPEN (for example, do not click on) the attachment. We need to rite down the e-mail address of the person it came from and then delete the message. Then we can send a note to the sender so that they know that their computer has been infected.

File Signature validation

We have checked the binary file for the selected malware in hexed.it. We have considered the first few bytes for signature validation. Below is the snapshot of the webpage :



File Information

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

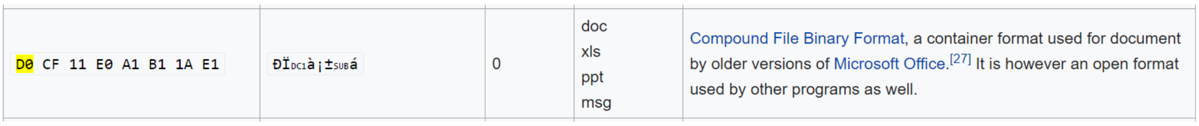
Data Inspector (Little-endian)

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	2023-02-14 15:54:56 Local	
Macintosh HFS+ DateTime	2023-02-14 23:54:56 UTC	
Binary	● ● ○ ● ○ ○ ○ ○	

Data Inspector (Big-endian)

```
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
000001B0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001C0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001D0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001E0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001F0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000200  EC A5 C1 00 7F 60 15 04 00 00 F0 12 BF 00 00 00  ∞Ñ┴.⌂`....≡.┐...
00000210  00 00 00 10 00 00 00 00 00 06 00 00 26 2B 00 00  ............&+..
```

Validating file signature from Wikipedia file signature scheme:

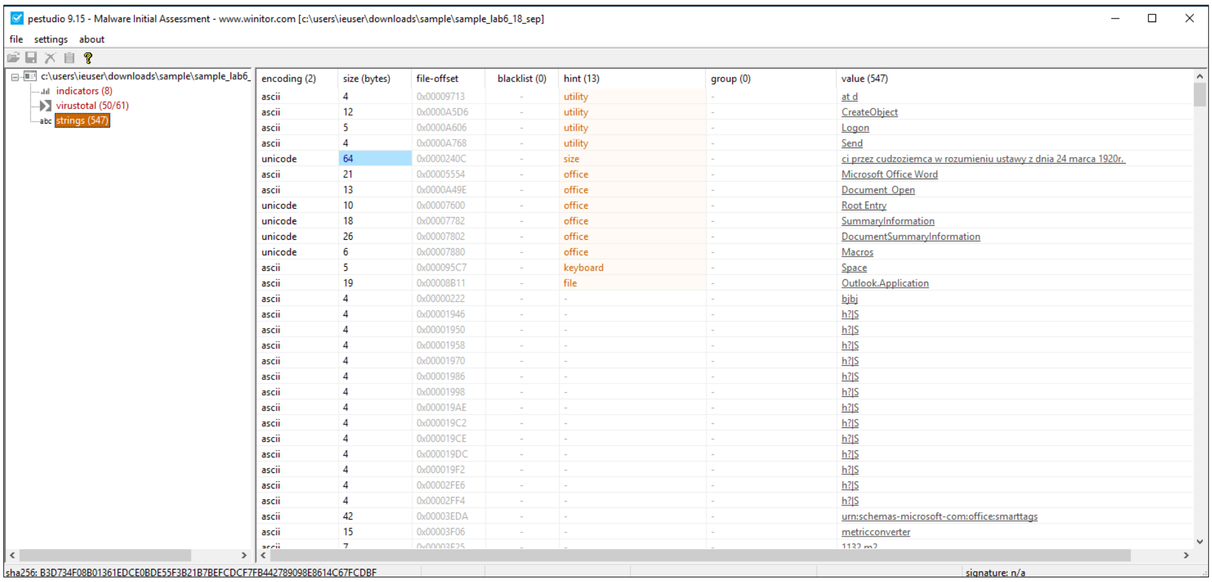


D0 CF 11 E0 A1 B1 1A E1	ÐÏ␑à¡±␚á	0	doc xls ppt msg	Compound File Binary Format, a container format used for document by older versions of Microsoft Office.[27] It is however an open format used by other programs as well.

We can Assume the file to be any of the above file types. To get a clear-cut idea, we have checked other static analysis tools such as PEStudio, VirusTotal etc.

Static Analysis using PEStudio Tool

From this snapshot, we can confirm that the sample is Microsoft Office Word file.



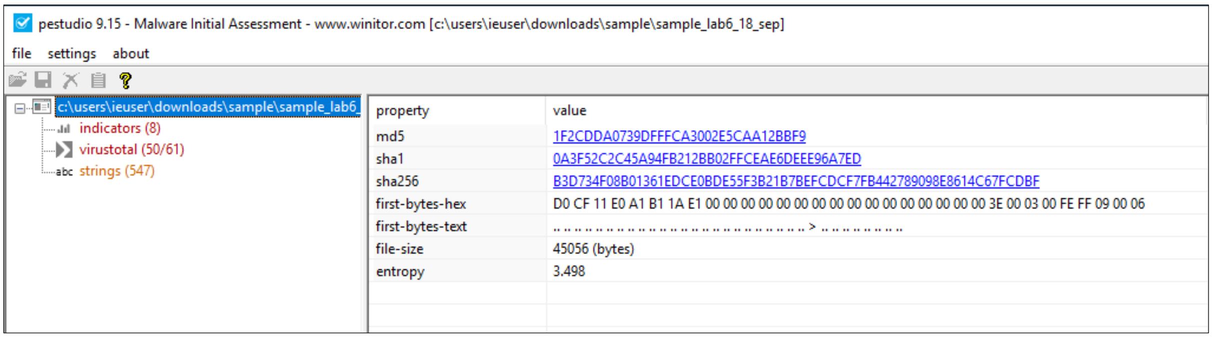
pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\ieuser\downloads\sample\sample_lab6_18_sep]

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	0x00002FE6	-	-	-	h?|S
ascii	4	0x00002FF4	-	-	-	h?|S
ascii	42	0x00003EDA	-	-	-	urn:schemas-microsoft-com:office:smarttags
ascii	15	0x00003F06	-	-	-	metricconverter
ascii	7	0x00003F25	-	-	-	1132 m2

sha256: B3D734F08B01361EDCE0BDE55F3B21B7BEFCDCF7FB442789098E8614C67FCDBF

signature: n/a

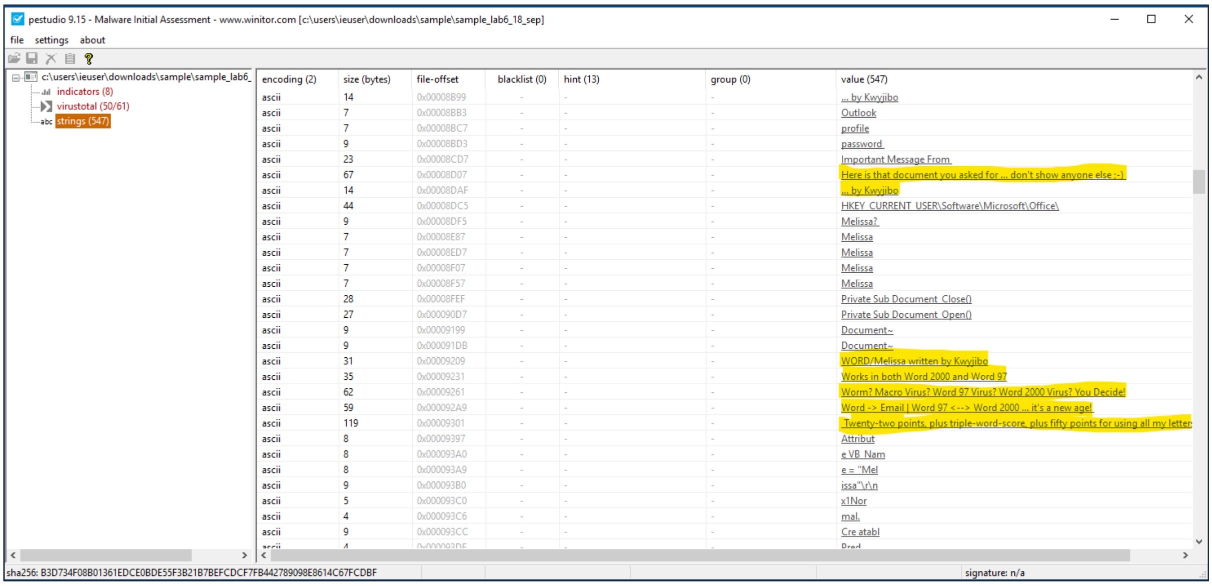
We can get an idea about the Hash Values, first bytes and entropy of the sample file as below



pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\ieuser\downloads\sample\sample_lab6_18_sep]

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

Here are few other strings which we are going to use while creating the Yara rule.



pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\ieuser\downloads\sample\sample_lab6_18_sep]

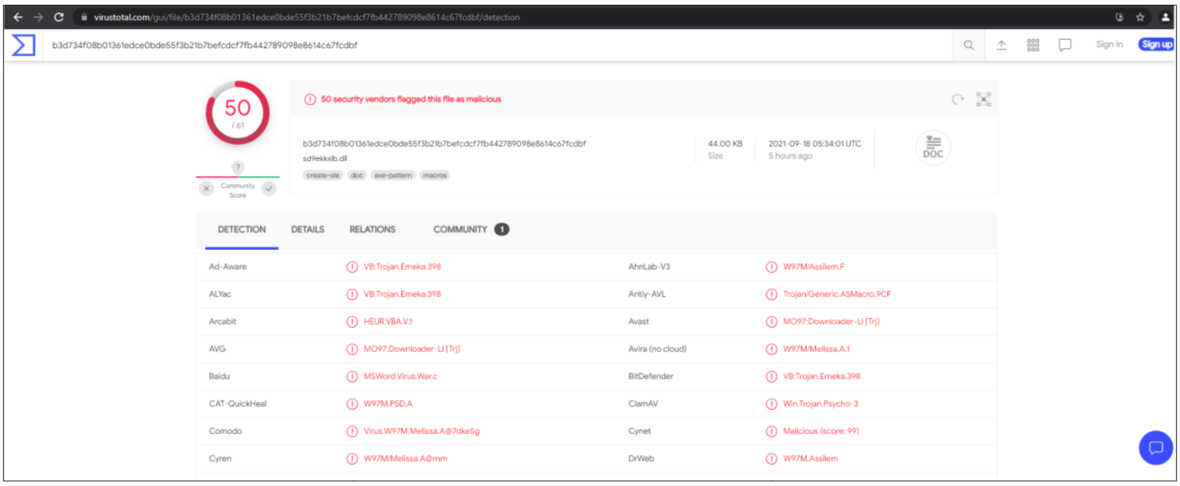
encoding (2)	size (bytes)	file-offset	blacklist (0)	hint (13)	group (0)	value (547)
ascii	14	0x00008B99	-	-	-	... by Kwyjibo
ascii	7	0x00008BB3	-	-	-	Outlook
ascii	7	0x00008BC7	-	-	-	profile
ascii	9	0x00008BD3	-	-	-	password
ascii	23	0x00008CD7	-	-	-	Important Message From
ascii	67	0x00008D07	-	-	-	Here 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
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 letter
ascii	8	0x00009397	-	-	-	Attribut
ascii	8	0x000093A0	-	-	-	e VB_Nam
ascii	8	0x000093A9	-	-	-	e = "Mel
ascii	9	0x000093B0	-	-	-	issa"\r\n
ascii	5	0x000093C0	-	-	-	x1Nor
ascii	4	0x000093C6	-	-	-	mal.
ascii	9	0x000093CC	-	-	-	Cre atabl
ascii	4	0x000093DE	-	-	-	Pred

sha256: B3D734F08B01361EDCE0BDE55F3B21B7BEFCDCF7FB442789098E8614C67FCDBF

signature: n/a

Static Analysis using VirusTotal

We can confirm the hash and file type from the below snapshots



virustotal.com/gui/file/b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf/detection

b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf

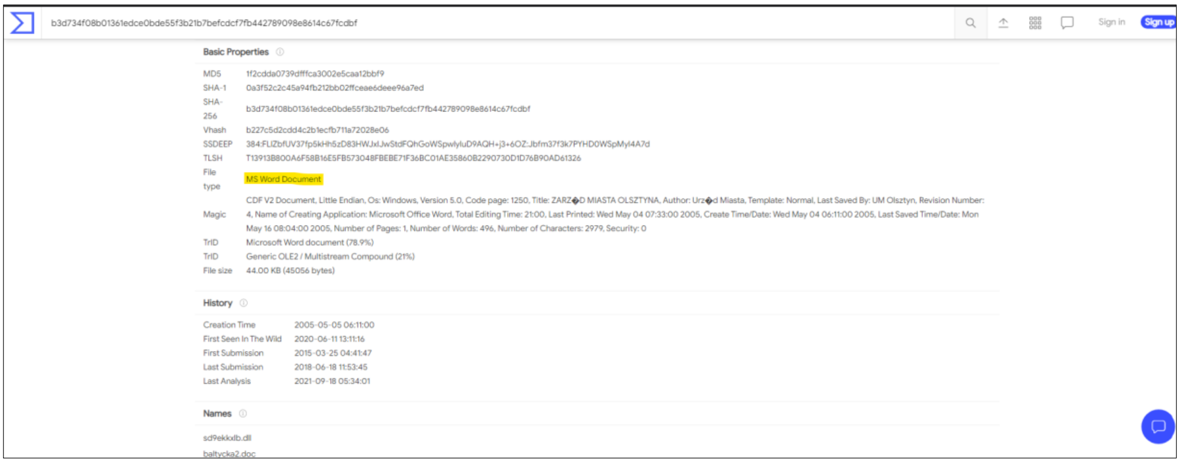
50 security vendors flagged this file as malicious

b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf
sd9ekkxlb.dll
create-ole doc exe-pattern macros

44.00 KB
Size

2021-09-18 05:34:01 UTC
5 hours ago

Ad-Aware	VB:Trojan.Emeka.398	AhnLab-V3	W97M/Assilem.F
ALYac	VB:Trojan.Emeka.398	Antiy-AVL	Trojan/Generic.ASMacro.9CF
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: 99)
Cyren	W97M/Melissa.A@mm	DrWeb	W97M.Assilem



b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf

Basic Properties

MD5	1f2cdda0739dfffca3002e5caa12bbf9
SHA-1	0a3f52c2c45a94fb212bb02ffceae6deee96a7ed
SHA-256	b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf
Vhash	b227c5d2cdd4c2b1ecfb711a72028e06
SSDEEP	384:FLIZbfUV37fp5kHh5zD83HWJxIJwStdFQhGoWSpwlyluD9AQH+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)

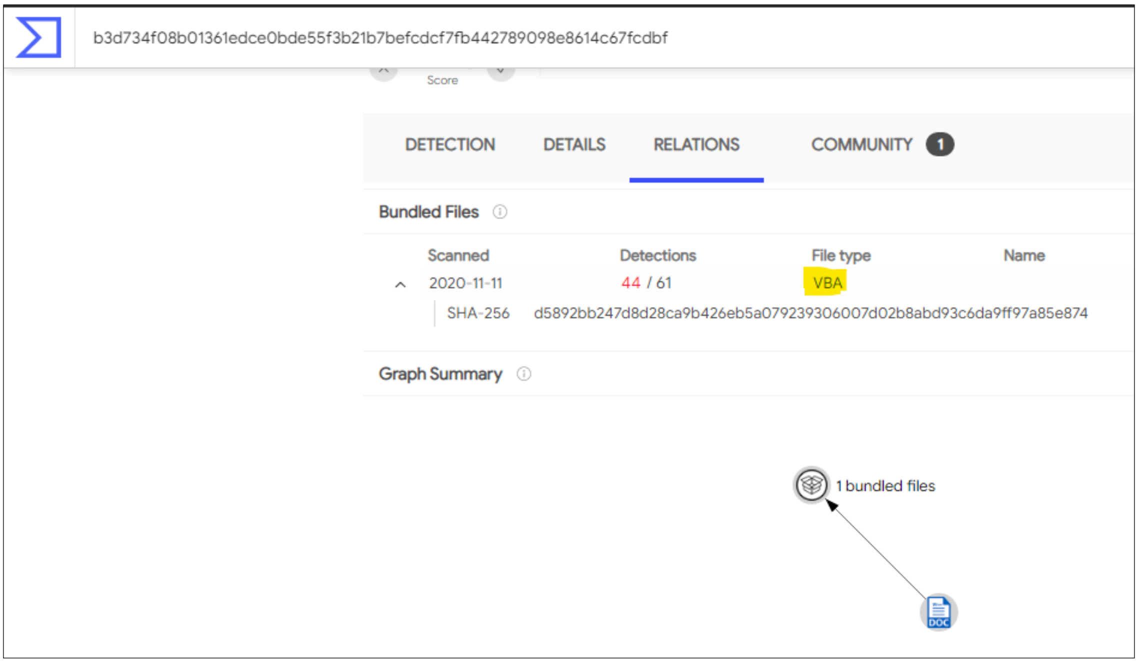
History

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	2021-09-18 05:34:01

Names

sd9ekkxlb.dll
baltycka2.doc

In the below snapshots, we can confirm that the sample file is using embedded macro (bundled VBA file).



b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf

Bundled Files

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

SHA-256 d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874

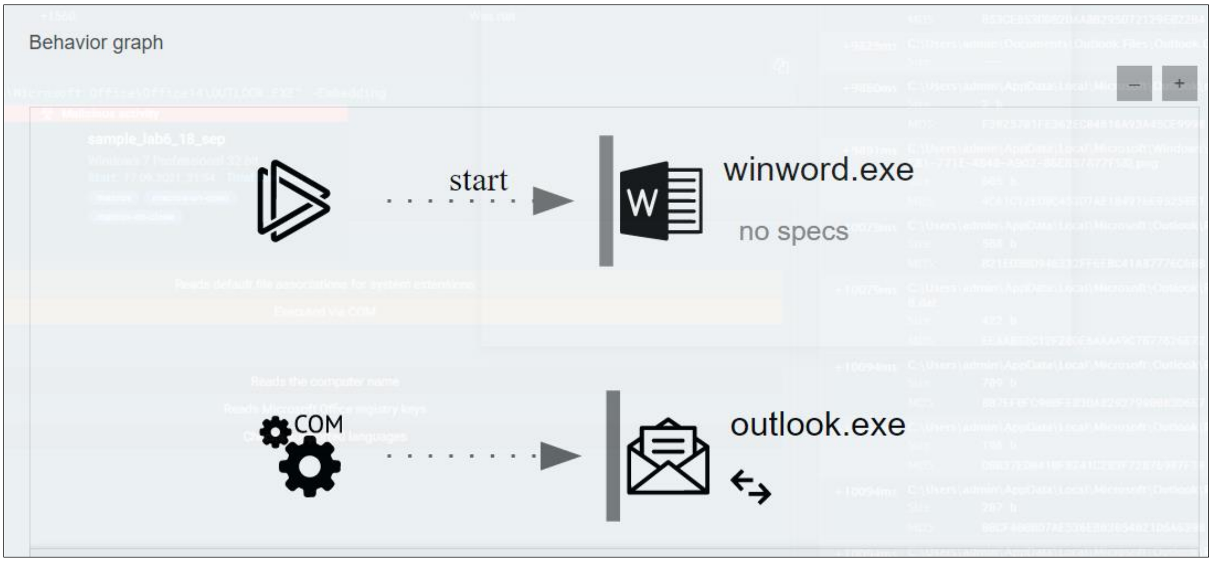
Graph Summary

Dynamic Analysis using Any.Run

The sample file has been run under sandboxed environment. Below are few details from the website: (Please note: currently the trial version allows the malware to run only for 1 minute).We have taken a few snapshots for analysis purpose.

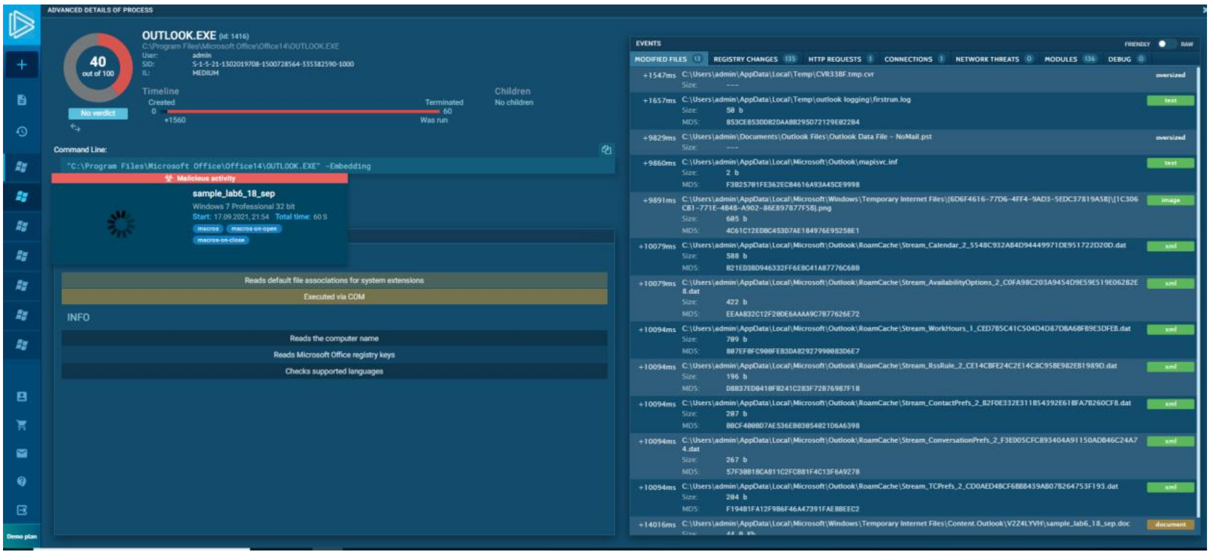
Behavior Graph

We can see that the word file is calling the embedded VBA macro script to open Outlook and then it will read the first 50 address in the address book and try to send the malicious code.



Process Graph

Here, it is clearly visible that the execution of outlook.exe has been listed as a warning and malicious activity.


ADVANCED DETAILS OF PROCESS

OUTLOOK.EXE (id: 1416)
C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE

User:	admin
SID:	S-1-5-21-1302019708-1500728564-335382590-1000
IL:	MEDIUM

40 out of 100

No verdict

Timeline
Created 0 +1560
Terminated 60 Was run

Children
No children

Command Line:

```
"C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE" -Embedding
```

Malicious activity

sample_lab6_18_sep
Windows 7 Professional 32 bit
Start: 17.09.2021, 21:54 Total time: 60 S
macros macros-on-open macros-on-close

Reads default file associations for system extensions

Executed via COM

INFO

Reads the computer name

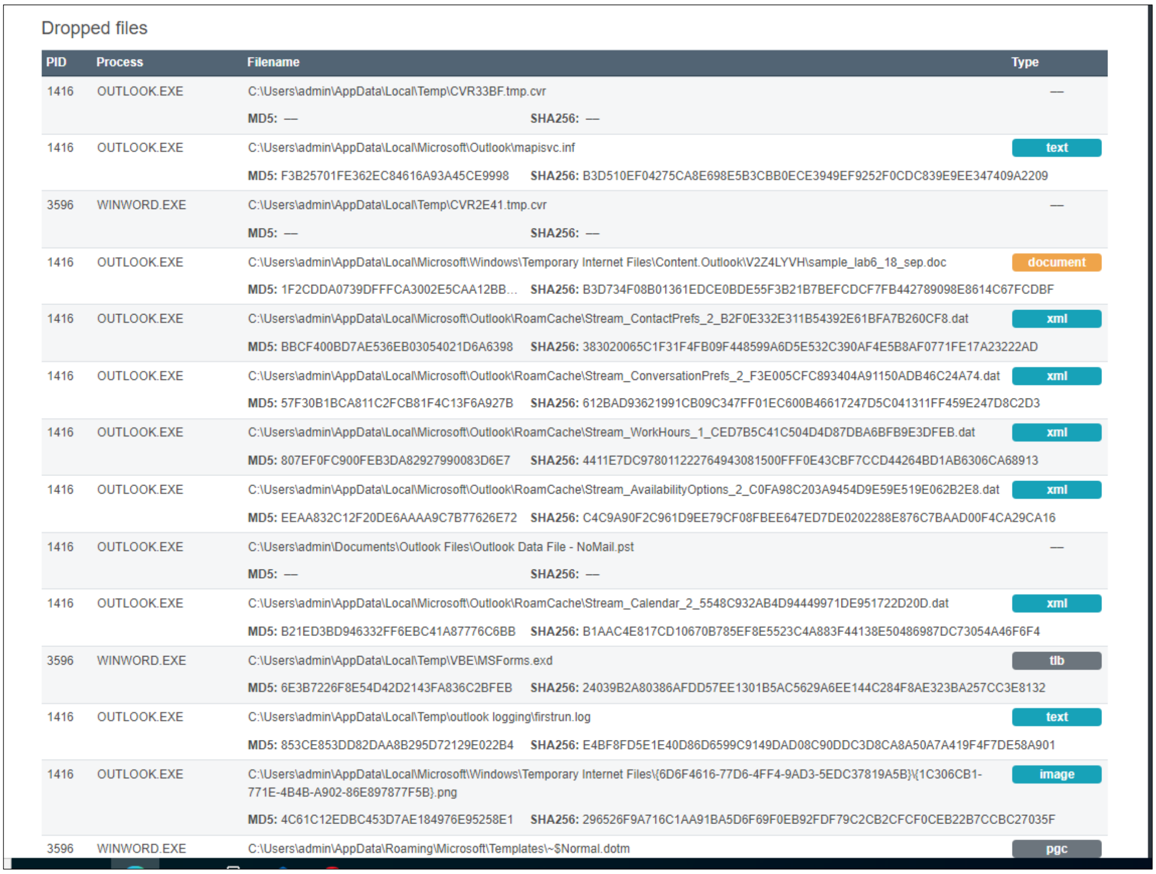
Reads Microsoft Office registry keys

Checks supported languages

EVENTS

```
+1547ms  C:\Users\admin\AppData\Local\Temp\CVR338F.tmp.cvr                                   oversized
         Size:   ---
+1657ms  C:\Users\admin\AppData\Local\Temp\outlook logging\firstrun.log                      text
         Size:   58 b
         MD5:    853CE853DD82DAA88295D72129E822B4
+9829ms  C:\Users\admin\Documents\Outlook Files\Outlook Data File - NoMail.pst               oversized
         Size:   ---
+9860ms  C:\Users\admin\AppData\Local\Microsoft\Outlook\mapisvc.inf                          text
         Size:   2 b
         MD5:    F3B25701FE362EC84616A93A45CE9998
+9891ms  C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\{6D6F4616-77D6-4FF4-9AD3-5EDC37819A58}\{1C306
         C81-771E-4848-A902-86E897877F58}.png                                                image
         Size:   605 b
         MD5:    4C61C12EDBC453D7AE184976E95258E1
+10079ms C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_Calendar_2_5548C932A84D94449971DE951722D20D.dat   xml
         Size:   588 b
         MD5:    821ED38D946332FF6E8C41A87776C688
+10079ms C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_AvailabilityOptions_2_C0FA98C203A9454D9E59E519E062B2E
         8.dat                                                                               xml
         Size:   422 b
         MD5:    EEAA832C12F28DE6AAAA9C7B77626E72
+10094ms C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_WorkHours_1_CED7B5C41C504D4D87DBA68FB9E3DFEB.dat   xml
         Size:   709 b
         MD5:    807EFBFC900FEB3DA82927990083D6E7
+10094ms C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_RssRule_2_CE14CBFE24C2E14C8C958E982EB1989D.dat   xml
         Size:   196 b
         MD5:    D8B37ED8410FB241C283F72B76987F18
+10094ms C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_ContactPrefs_2_82F0E332E311B54392E61BFA7B260CF8.dat   xml
         Size:   287 b
         MD5:    8BCF4000D7AE536EB83054021D6A6398
+10094ms C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_ConversationPrefs_2_F3E005CFC893404A91150ADB46C24A7
         4.dat                                                                               xml
         Size:   267 b
         MD5:    57F38818CA811C2FC881F4C13F6A9278
+10094ms C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_TCPrefs_2_CD0AED48CF6888439A807B264753F193.dat   xml
         Size:   284 b
         MD5:    F19481FA12F986F46A47391FAE88EEC2
+14016ms C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\V2Z4LYVH\sample_lab6_18_sep.doc   document
         Size:   44.0 Kb
```

Dropped Files



Dropped files

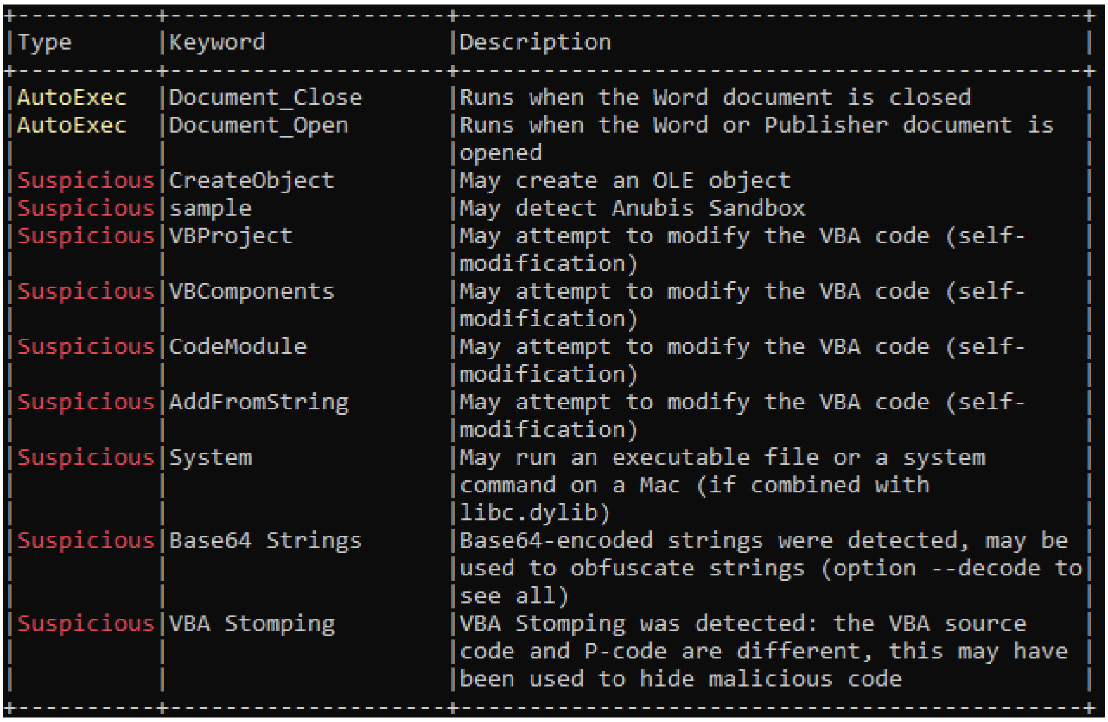
PID	Process	Filename	Type
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Temp\CVR33BF.tmp.cvr **MD5:** — **SHA256:** —	—
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Outlook\mapisvc.inf **MD5:** F3B25701FE362EC84616A93A45CE9998 **SHA256:** B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209	text
3596	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\CVR2E41.tmp.cvr **MD5:** — **SHA256:** —	—
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\V2Z4LYVH\sample_lab6_18_sep.doc **MD5:** 1F2CDDA0739DFFFCA3002E5CAA12BB... **SHA256:** B3D734F08B01361EDCE0BDE55F3B21B7BEFCDCF7FB442789098E8614C67FCDBF	document
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_ContactPrefs_2_B2F0E332E311B54392E61BFA7B260CF8.dat **MD5:** BBCF400BD7AE536EB03054021D6A6398 **SHA256:** 383020065C1F31F4FB09F448599A6D5E532C390AF4E5B8AF0771FE17A23222AD	xml
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_ConversationPrefs_2_F3E005CFC893404A91150ADB46C24A74.dat **MD5:** 57F30B1BCA811C2FCB81F4C13F6A927B **SHA256:** 612BAD93621991CB09C347FF01EC600B46617247D5C041311FF459E247D8C2D3	xml
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_WorkHours_1_CED7B5C41C504D4D87DBA6BFB9E3DFEB.dat **MD5:** 807EF0FC900FEB3DA82927990083D6E7 **SHA256:** 4411E7DC97801122276494308150 0FFF0E43CBF7CCD44264BD1AB6306CA68913	xml
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_AvailabilityOptions_2_C0FA98C203A9454D9E59E519E062B2E8.dat **MD5:** EEAA832C12F20DE6AAAA9C7B77626E72 **SHA256:** C4C9A90F2C961D9EE79CF08FBEE647ED7DE0202288E876C7BAAD00F4CA29CA16	xml
1416	OUTLOOK.EXE	C:\Users\admin\Documents\Outlook Files\Outlook Data File - NoMail.pst **MD5:** — **SHA256:** —	—
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_Calendar_2_5548C932AB4D94449971DE951722D20D.dat **MD5:** B21ED3BD946332FF6EBC41A87776C6BB **SHA256:** B1AAC4E817CD10670B785EF8E5523C4A883F44138E50486987DC73054A46F6F4	xml
3596	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\VBE\MSForms.exd **MD5:** 6E3B7226F8E54D42D2143FA836C2BFEB **SHA256:** 24039B2A80386AFDD57EE1301B5AC5629A6EE144C284F8AE323BA257CC3E8132	tlb
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Temp\outlook logging\firstrun.log **MD5:** 853CE853DD82DAA8B295D72129E022B4 **SHA256:** E4BF8FD5E1E40D86D6599C9149DAD08C90DDC3D8CA8A50A7A419F4F7DE58A901	text
1416	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\{6D6F4616-77D6-4FF4-9AD3-5EDC37819A5B}\{1C306CB1-771E-4B4B-A902-86E897877F5B}.png **MD5:** 4C61C12EDBC453D7AE184976E95258E1 **SHA256:** 296526F9A716C1AA91BA5D6F69F0EB92FDF79C2CB2CFCF0CEB22B7CCBC27035F	image
3596	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	pgc

Below is the execution report and full analysis link of ANY.RUN website:

https://any.run/report/47f4d62c59b9643f5dbb6d7447570ed98ccd77e0ef77e5ba870e3b978ae8fec5/1009cc31-902e-4bc7-8aa0-893aefde09e8#screenshots

Dynamic Analysis using Olevba Tool

Olevba tool has been used to perform dynamic analysis of the selected malware sample in flare VM environment and snapshot of Execution report generated is as below :



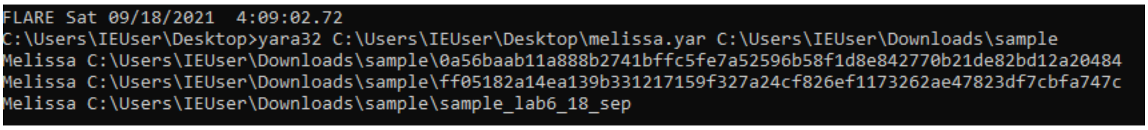
```
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |Document_Close      |Runs when the Word document is closed        |
|AutoExec  |Document_Open       |Runs when the Word or Publisher document is  |
|          |                    |opened                                       |
|Suspicious|CreateObject        |May create an OLE object                     |
|Suspicious|sample              |May detect Anubis Sandbox                    |
|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             |
+----------+--------------------+---------------------------------------------+
```

Below is the full report from InQuest Lab Deep File Inspection (DFI):
https://labs.inquest.net/dfi/hash/b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf

YARA Rule Execution

Yara Rule has been uploaded in GitHub (https://github.com/SayanKantiMukherjee/ThreatIntelligenceLab/blob/main/Lab_6_Melissa_Malware/Melissa_Malware_Yara_Rule.yara)

Below is the execution in flare VM with samples:



```
FLARE Sat 09/18/2021  4:09:02.72
C:\Users\IEUser\Desktop>yara32 C:\Users\IEUser\Desktop\melissa.yar C:\Users\IEUser\Downloads\sample
Melissa C:\Users\IEUser\Downloads\sample\0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484
Melissa C:\Users\IEUser\Downloads\sample\ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c
Melissa C:\Users\IEUser\Downloads\sample\sample_lab6_18_sep
```

Reference

1) https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519
2) https://searchsecurity.techtarget.com/definition/Melissa-virus
3) https://www.f-secure.com/v-descs/melissa.shtml