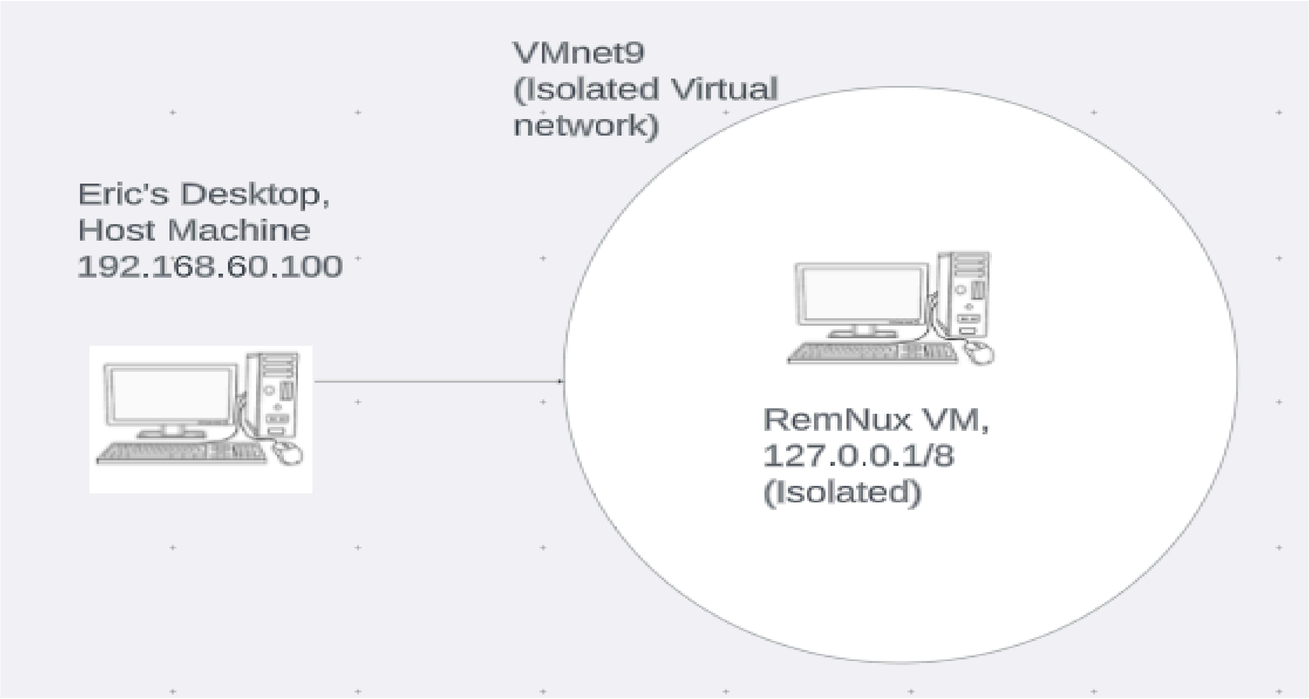
Eric Guzman 11/22/2023
Professor Cannistra Network Security

Lab 5

Description: In this lab we used our Kali Linux VM to use active discovery techniques and tools on a Metasploitable Linux VM.

Topology:



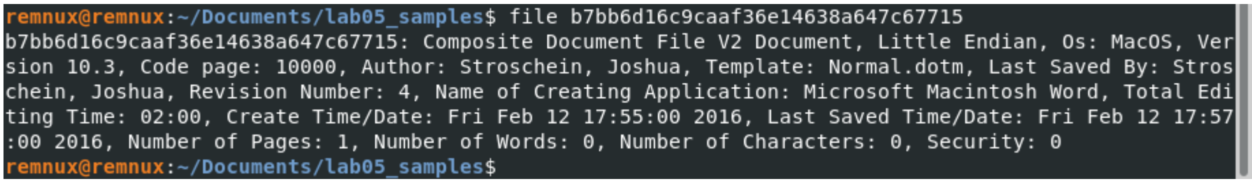
Syntax:

Command	**Syntax**
Oledump.py doc	Analyzes the doc for certain data
Oledump.py -s 7 doc	Displays the content of stream 7
Oledump.py -s 8 -d doc > newdoc.txt	Decodes and extracts stream 8's content to a text file

Verification:

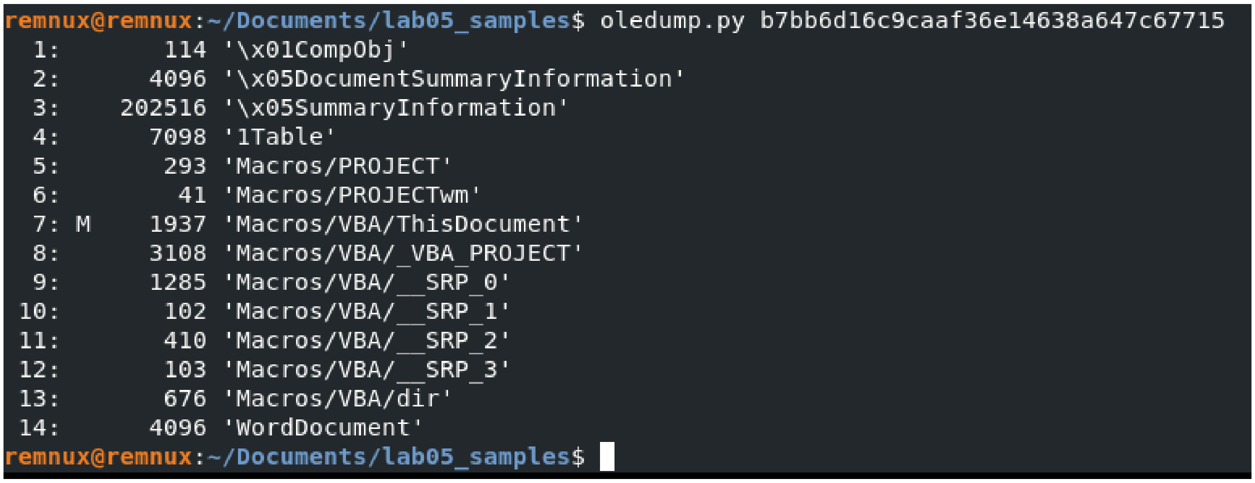
File 1:

b. This screenshot shows the results of using the file utility -



```
remnux@remnux:~/Documents/lab05_samples$ file b7bb6d16c9caaf36e14638a647c67715
b7bb6d16c9caaf36e14638a647c67715: Composite Document File V2 Document, Little Endian, Os: MacOS, Ver
sion 10.3, Code page: 10000, Author: Stroschein, Joshua, Template: Normal.dotm, Last Saved By: Stros
chein, Joshua, Revision Number: 4, Name of Creating Application: Microsoft Macintosh Word, Total Edi
ting Time: 02:00, Create Time/Date: Fri Feb 12 17:55:00 2016, Last Saved Time/Date: Fri Feb 12 17:57
:00 2016, Number of Pages: 1, Number of Words: 0, Number of Characters: 0, Security: 0
remnux@remnux:~/Documents/lab05_samples$
```

c. This screenshot shows the results of using the general results of oledump.py utility -



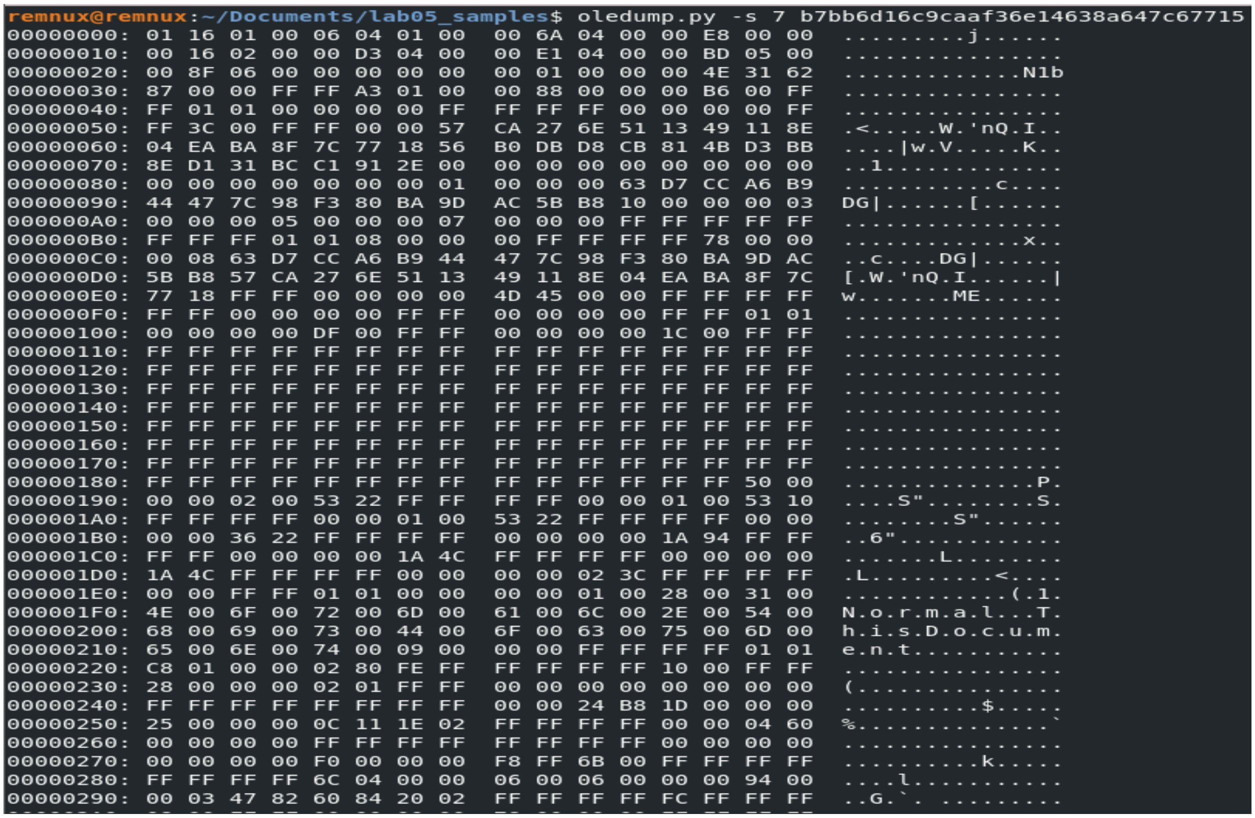
```
remnux@remnux:~/Documents/lab05_samples$ oledump.py b7bb6d16c9caaf36e14638a647c67715
  1:       114 '\x01CompObj'
  2:      4096 '\x05DocumentSummaryInformation'
  3:    202516 '\x05SummaryInformation'
  4:      7098 '1Table'
  5:       293 'Macros/PROJECT'
  6:        41 'Macros/PROJECTwm'
  7: M    1937 'Macros/VBA/ThisDocument'
  8:      3108 'Macros/VBA/_VBA_PROJECT'
  9:      1285 'Macros/VBA/__SRP_0'
 10:       102 'Macros/VBA/__SRP_1'
 11:       410 'Macros/VBA/__SRP_2'
 12:       103 'Macros/VBA/__SRP_3'
 13:       676 'Macros/VBA/dir'
 14:      4096 'WordDocument'
remnux@remnux:~/Documents/lab05_samples$
```

i. Yes, this file contains macros.

ii. Files like: Macros/PROJECT, Macros/VBA/ThisDocument, and Macros/VBA/_VBA_PROJECT all have the word macro in their name, leading me to believe that they contain macros. One file is also marked with a “M”, showing it is a stream that may contain something interesting.

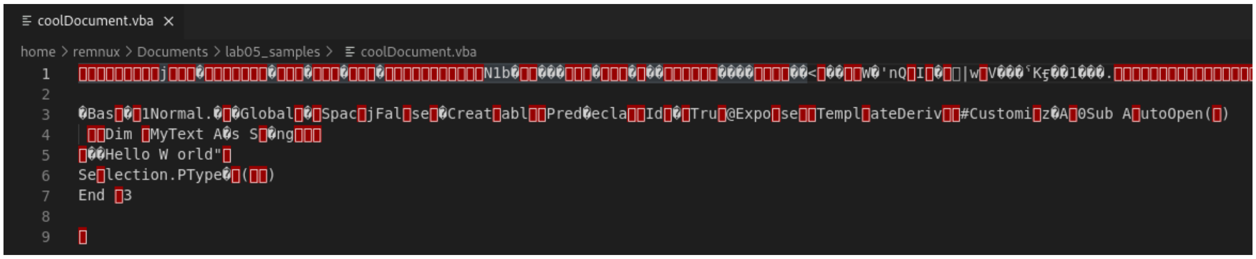
iii. The streams that may contain macros are Macros/PROJECT, Macros/PROJECTwm, Macros/VBA/ThisDocument, Macros/VBA/_VBA_PROJECT, Macros/VBA/__SRP_0, Macros/VBA/__SRP_1, Macros/VBA/__SRP_2, Macros/VBA/__SRP_3, Macros/VBA/dir.

iv. This screenshot shows inspecting the stream of Macros/VBA/ThisDocument in a hexdump using the command oledump.py -s 7 b7bb6d16c9caaf36e14638a647c67715.



```
remnux@remnux:~/Documents/lab05_samples$ oledump.py -s 7 b7bb6d16c9caaf36e14638a647c67715
00000000: 01 16 01 00 06 04 01 00  00 6A 04 00 00 E8 00 00  .........j......
00000010: 00 16 02 00 00 D3 04 00  00 E1 04 00 00 BD 05 00  ................
00000020: 00 8F 06 00 00 00 00 00  00 01 00 00 00 4E 31 62  .............N1b
00000030: 87 00 00 FF FF A3 01 00  00 88 00 00 00 B6 00 FF  ................
00000040: FF 01 01 00 00 00 00 FF  FF FF FF 00 00 00 00 FF  ................
00000050: FF 3C 00 FF FF 00 00 57  CA 27 6E 51 13 49 11 8E  .<.....W.'nQ.I..
00000060: 04 EA BA 8F 7C 77 18 56  B0 DB D8 CB 81 4B D3 BB  ....|w.V.....K..
00000070: 8E D1 31 BC C1 91 2E 00  00 00 00 00 00 00 00 00  ..1.............
00000080: 00 00 00 00 00 00 00 01  00 00 00 63 D7 CC A6 B9  ...........c....
00000090: 44 47 7C 98 F3 80 BA 9D  AC 5B B8 10 00 00 00 03  DG|......[......
000000A0: 00 00 00 05 00 00 00 07  00 00 00 FF FF FF FF FF  ................
000000B0: FF FF FF 01 01 08 00 00  00 FF FF FF FF 78 00 00  .............x..
000000C0: 00 08 63 D7 CC A6 B9 44  47 7C 98 F3 80 BA 9D AC  ..c....DG|......
000000D0: 5B B8 57 CA 27 6E 51 13  49 11 8E 04 EA BA 8F 7C  [.W.'nQ.I......|
000000E0: 77 18 FF FF 00 00 00 00  4D 45 00 00 FF FF FF FF  w.......ME......
000000F0: FF FF 00 00 00 00 FF FF  00 00 00 00 FF FF 01 01  ................
00000100: 00 00 00 00 DF 00 FF FF  00 00 00 00 1C 00 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 FF FF FF FF FF FF  ................
00000180: FF FF FF FF FF FF FF FF  FF FF FF FF FF FF 50 00  ..............P.
00000190: 00 00 02 00 53 22 FF FF  FF FF 00 00 01 00 53 10  ....S"........S.
000001A0: FF FF FF FF 00 00 01 00  53 22 FF FF FF FF 00 00  ........S"......
000001B0: 00 00 36 22 FF FF FF FF  00 00 00 00 1A 94 FF FF  ..6"............
000001C0: FF FF 00 00 00 00 1A 4C  FF FF FF FF 00 00 00 00  .......L........
000001D0: 1A 4C FF FF FF FF 00 00  00 00 02 3C FF FF FF FF  .L.........<....
000001E0: 00 00 FF FF 01 01 00 00  00 00 01 00 28 00 31 00  ............(.1.
000001F0: 4E 00 6F 00 72 00 6D 00  61 00 6C 00 2E 00 54 00  N.o.r.m.a.l...T.
00000200: 68 00 69 00 73 00 44 00  6F 00 63 00 75 00 6D 00  h.i.s.D.o.c.u.m.
00000210: 65 00 6E 00 74 00 09 00  00 00 FF FF FF FF 01 01  e.n.t...........
00000220: C8 01 00 00 02 80 FE FF  FF FF FF FF 10 00 FF FF  ................
00000230: 28 00 00 00 02 01 FF FF  00 00 00 00 00 00 00 00  (...............
00000240: FF FF FF FF FF FF FF FF  00 00 24 B8 1D 00 00 00  ..........$.....
00000250: 25 00 00 00 0C 11 1E 02  FF FF FF FF 00 00 04 60  %..............`
00000260: 00 00 00 00 FF FF FF FF  FF FF FF FF 00 00 00 00  ................
00000270: 00 00 00 00 F0 00 00 00  F8 FF 6B 00 FF FF FF FF  ..........k.....
00000280: FF FF FF FF 6C 04 00 00  06 00 06 00 00 00 94 00  ....l...........
00000290: 00 03 47 82 60 84 20 02  FF FF FF FF FC FF FF FF  ..G.`. .........
```

v. I attempted to extract the stream of Macros/VBA/ThisDocument into VSCode on the VM and got very obfuscated code.



coolDocument.vba ×
home > remnux > Documents > lab05_samples > coolDocument.vba

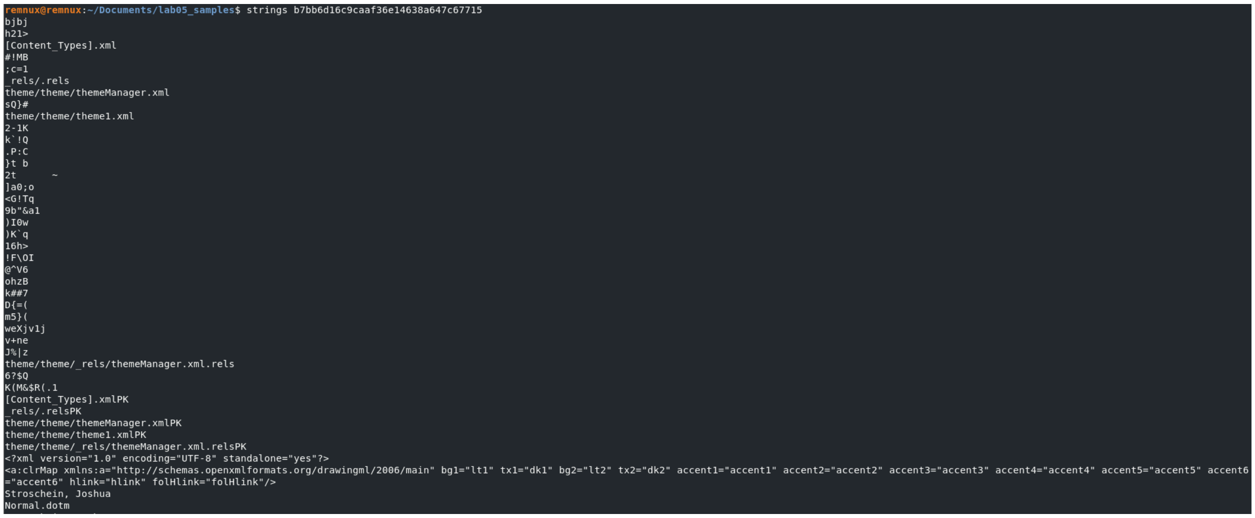
```
▯▯▯▯▯▯▯▯▯j▯▯▯�▯▯▯▯▯▯▯▯�▯▯▯�▯▯▯�▯▯▯�▯▯▯▯▯▯▯▯▯▯▯▯N1b�▯▯���▯▯▯�▯▯▯�▯��▯▯▯▯▯▯▯����▯▯▯▯▯��<▯��▯▯W�'nQ▯I▯�▯▯|w▯V���ˁKƺ��1���.▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯

�Bas▯�▯1Normal.�▯�Global▯�▯Spac▯jFal▯se▯�Creat▯abl▯▯Pred�ecla▯▯Id▯�▯Tru▯@Expo▯se▯▯Templ▯ateDeriv▯▯#Customi▯z�A▯0Sub A▯utoOpen(▯)
 ▯▯Dim ▯MyText A�s S▯�ng▯▯▯
▯��Hello W orld"▯
Se▯lection.PType�▯(▯▯)
End ▯3

▯
```

Vi. Some potential IOCs I can see here are ExposeTemplateDeriv, and AutoOpen().

Vii. Yes, I think this file is malicious.

Viii. I think this file is malicious because from what I can see the macro is automatically opening itself, which may not be inherently bad, but I am unable to see much else of the code making it hard to determine if the rest of the macro can be safe.

d. This screenshot shows the results of using the strings utility to inspect the file.

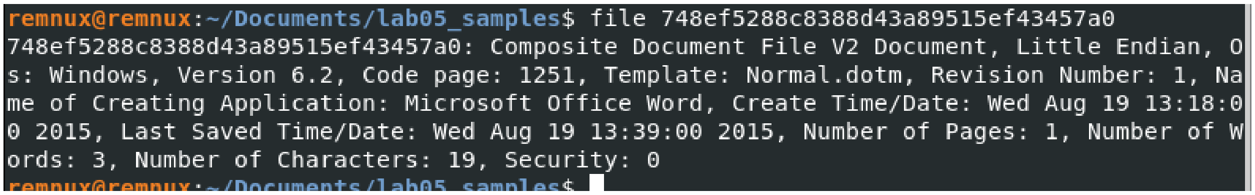


```
remnux@remnux:~/Documents/lab05_samples$ strings b7bb6d16c9caaf36e14638a647c67715
bjbj
h21>
[Content_Types].xml
#!MB
;c=1
_rels/.rels
theme/theme/themeManager.xml
sQ}#
theme/theme/theme1.xml
2-1K
k`!Q
.P:C
}t b
2t      ~
]a0;o
<G!Tq
9b"&a1
)I0w
)K`q
16h>
!F\OI
@^V6
ohzB
k##7
D{=(
m5}(
weXjv1j
v+ne
J%|z
theme/theme/_rels/themeManager.xml.rels
6?$Q
K(M&$R(.1
[Content_Types].xmlPK
_rels/.relsPK
theme/theme/themeManager.xmlPK
theme/theme/theme1.xmlPK
theme/theme/_rels/themeManager.xml.relsPK
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<a:clrMap xmlns:a="http://schemas.openxmlformats.org/drawingml/2006/main" bg1="lt1" tx1="dk1" bg2="lt2" tx2="dk2" accent1="accent1" accent2="accent2" accent3="accent3" accent4="accent4" accent5="accent5" accent6
="accent6" hlink="hlink" folHlink="folHlink"/>
Stroschein, Joshua
Normal.dotm
```

i. Some of the key strings and objects I found are Dim my text as Sng, Hello World, End 3, Selection.PType and Sub AutoOpen().
ii. I can see that Sub AutoOpen() is used in macros to have them automatically open up when the document does. Selection.PType may be used to change the current selection in the document.

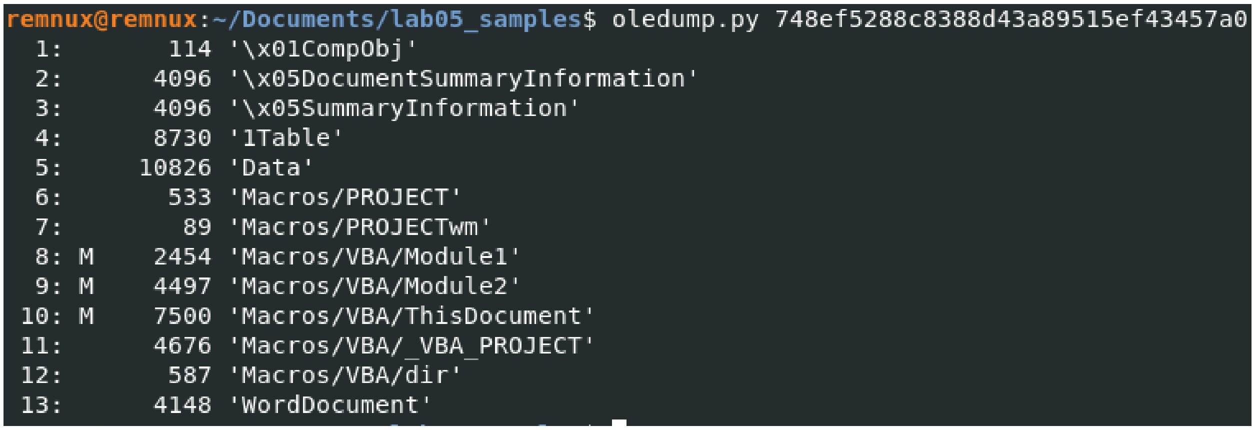
e.
i. Yeah this malware sample is doing a lot. The report made by hybrid analysis tells us that the malware is doing multiple things like: trying to steal mail credentials, spawning a lot of processes, queries process information, querying the display settings of system associated file extensions and more. I would have never found all of this by my own analysis.
ii. I am not sure what the command is doing here.

File 2:
B. This screenshot shows the results of using the file utility -



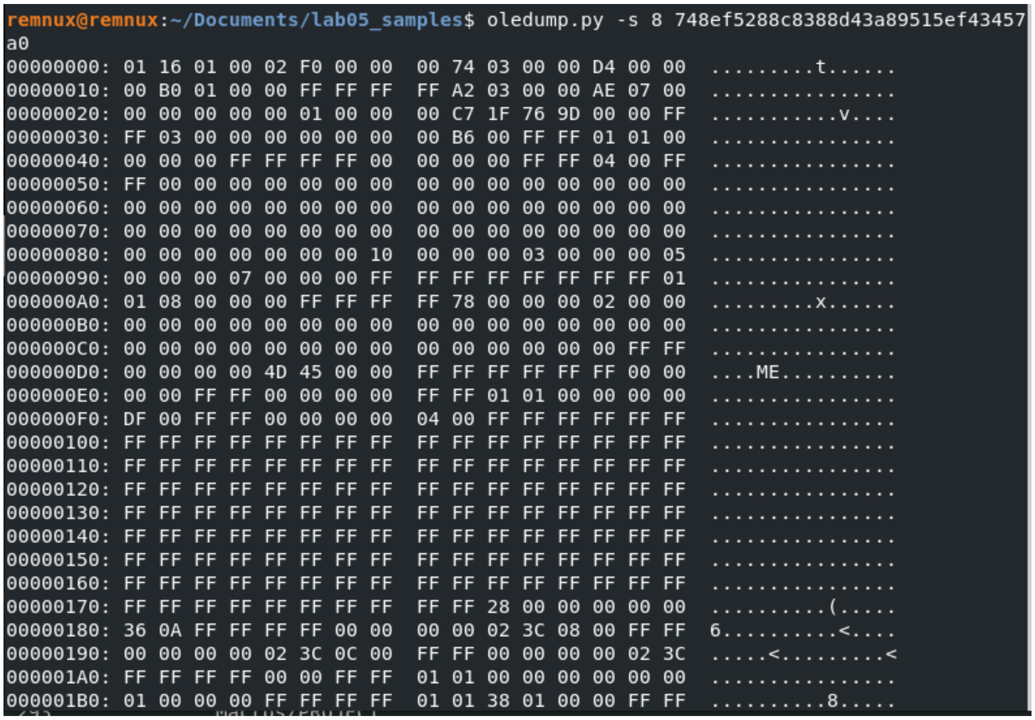
```
remnux@remnux:~/Documents/lab05_samples$ file 748ef5288c8388d43a89515ef43457a0
748ef5288c8388d43a89515ef43457a0: Composite Document File V2 Document, Little Endian, O
s: Windows, Version 6.2, Code page: 1251, Template: Normal.dotm, Revision Number: 1, Na
me of Creating Application: Microsoft Office Word, Create Time/Date: Wed Aug 19 13:18:0
0 2015, Last Saved Time/Date: Wed Aug 19 13:39:00 2015, Number of Pages: 1, Number of W
ords: 3, Number of Characters: 19, Security: 0
remnux@remnux:~/Documents/lab05_samples$
```

c. This screenshot shows the results of using the general results of oledump.py utility -



```
remnux@remnux:~/Documents/lab05_samples$ oledump.py 748ef5288c8388d43a89515ef43457a0
  1:       114 '\x01CompObj'
  2:      4096 '\x05DocumentSummaryInformation'
  3:      4096 '\x05SummaryInformation'
  4:      8730 '1Table'
  5:     10826 'Data'
  6:       533 'Macros/PROJECT'
  7:        89 'Macros/PROJECTwm'
  8: M    2454 'Macros/VBA/Module1'
  9: M    4497 'Macros/VBA/Module2'
 10: M    7500 'Macros/VBA/ThisDocument'
 11:      4676 'Macros/VBA/_VBA_PROJECT'
 12:       587 'Macros/VBA/dir'
 13:      4148 'WordDocument'
```

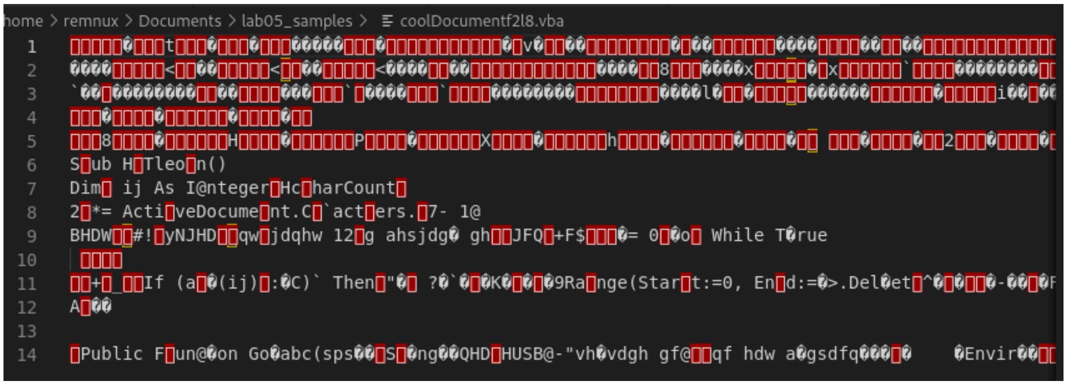
i. Yes, this file contains macros.
ii. Files like: Macros/PROJECT, Macros/VBA/ThisDocument, and Macros/VBA/_VBA_PROJECT all have the word macro in their name, leading me to believe that they contain macros. A few files are also marked with a “M”, showing it is a stream that may contain something interesting.
iii. The streams that may contain macros are Macros/PROJECT, Macros/PROJECTwm, Macros/VBA/Module1, Macros/VBA/Module2, Macros/VBA/ThisDocument, Macros/VBA/_VBA_PROJECT, Macros/VBA/dir.
iv. This screenshot shows inspecting the stream of Macros/VBA/Module1 in a hexdump using the command oledump.py -s 8 748ef5288c8388d43a89515ef43457a0



```
remnux@remnux:~/Documents/lab05_samples$ oledump.py -s 8 748ef5288c8388d43a89515ef43457
a0
00000000: 01 16 01 00 02 F0 00 00  00 74 03 00 00 D4 00 00  .........t......
00000010: 00 B0 01 00 00 FF FF FF  FF A2 03 00 00 AE 07 00  ................
00000020: 00 00 00 00 00 01 00 00  00 C7 1F 76 9D 00 00 FF  ...........v....
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  04 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: 36 0A FF FF FF FF 00 00  00 00 02 3C 08 00 FF FF  6.........<....
00000190: 00 00 00 00 02 3C 0C 00  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  ................
000001B0: 01 00 00 00 FF FF FF FF  01 01 38 01 00 00 FF FF  ..........8.....
```

v. I attempted to extract the streams of Macros/VBA/Module1, Macros/VBA/Module2, Macros/VBA/ThisDocument into VSCode on the VM and got very obfuscated code.

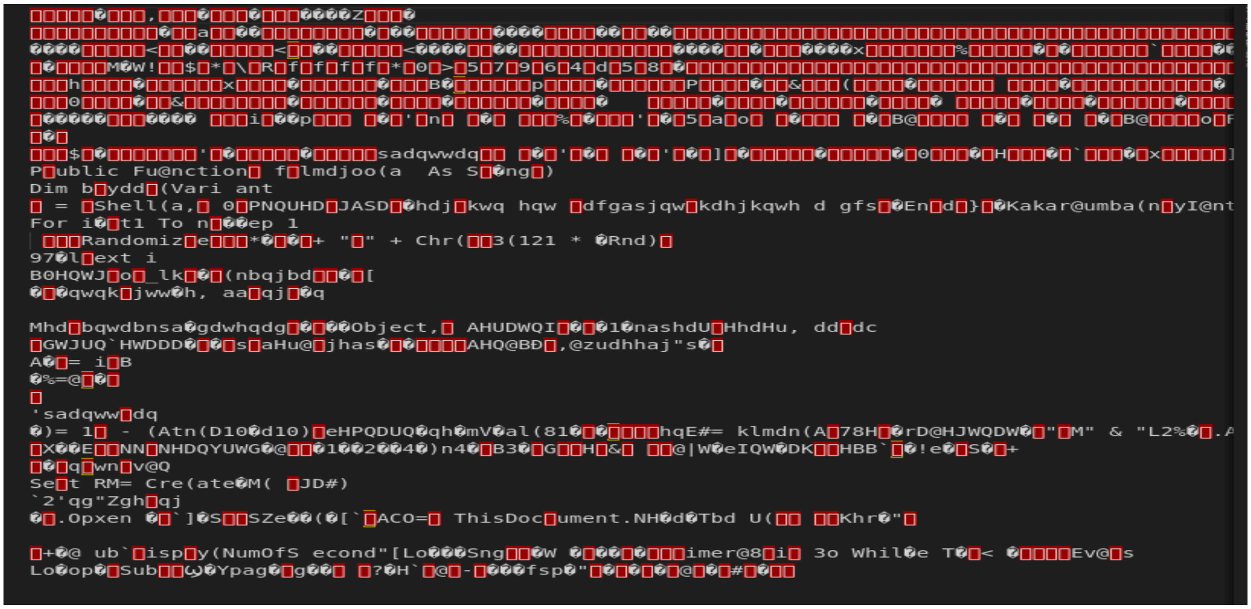
Macros/VBA/Module1 -



home > remnux > Documents > lab05_samples > coolDocumentf2l8.vba

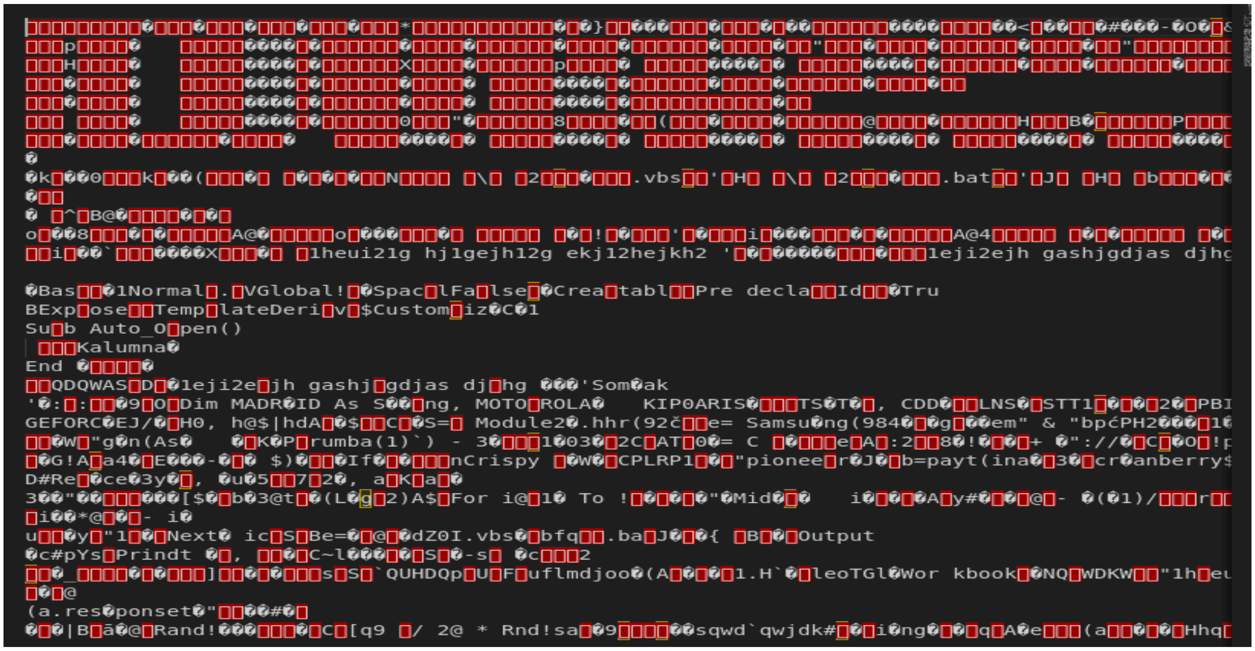
```
□□□□□�□□□t□□□�□□□�□□□�����□□□�□□□□□□□□□□□□�□v�□□��□□□□□□□□□�□��□□□□□□����□□□□��□□��□□□□□□□□□□□□□
����□□□□□<□□��□□□□□<□□��□□□□□<����□□��□□□□□□□□□□□□□����□□8□□□����x□□□□�□x□□□□□□`□□□□��������□□
`��□���������□□��□□□□���□□□`□�����□□□`□□□□��������□□□□□□□□□□����l�□□�□□□□□������□□□□□□�□□□□□i��□��
□□□�□□□□�□□□□□□□�□□□□�□□
□□□8□□□□�□□□□□□□H□□□□�□□□□□□□P□□□□�□□□□□□□X□□□□�□□□□□□□h□□□□�□□□□□□□�□□□□�□□ □□□�□□□□�□□2□□□�□□□□�□
S□ub H□Tleo□n()
Dim□ ij As I@nteger□Hc□harCount□
2□*= Acti□veDocume□nt.C□`act□ers.□7- 1@
BHDW□□#!□yNJHD□□qw□jdqhw 12□g ahsjdg� gh□□JFQ□+F$□□□�= 0□�o□ While T�rue
 □□□□
□□+□_□□If (a□�(ij)□:�C)` Then□"�□ ?�`�□�K�□�□�9Ra□nge(Star□t:=0, En□d:=�>.Del�et□^�□�□□�-��□�F
A□��

□Public F□un@�on Go�abc(sps��□S□�ng��QHD□HUSB@-"vh�vdgh gf@□□qf hdw a�gsdfq���□�    �Envir��□□
```

Macros/VBA/Module2



```
□□□□□�□□□,□□□�□□□�□□□����Z□□□�
□□□□□□□□□□�□□a□□��□□□□□□□□□�□��□□□□□□□����□□□□��□□��□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
����□□□□□<□□��□□□□□<□□��□□□□□<����□□��□□□□□□□□□□□□□����□□�□□□����x□□□□□□□%□□□□□�□�□□□□□□`□□□□��
□�□□□□M�W!□□$□*□\□R□f□f□f□f□*□0□>□5□7□9□6□4□d□5□8□�□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□h□□□□□�□□□□□□□x□□□□□�□□□□□□□�□□□□B�□□□□□□□p□□□□□�□□□□□□P□□□□□�□□&□□□(□□□□□�□□□□□□□ □□□□□�□□□□□□□□□□□□□□�
□□□0□□□□□�□□&□□□□□□□□□�□□□□□□□�□□□□□�□□□□□□□�□□□□□�   □□□□□□�□□□□□�□□□□□□□�□□□□□� □□□□□□�□□□□□�□□□□□□□�□□□□
□������□□□□���� □□□i□��p□□□ □�□'□n□ □�□ □□□%□�□□□'□�□5□a□o□ □�□□□ □�□B@□□□□ □�□ □�□ □�□B@□□□□o□F
□�□
□□□$□�□□□□□□□□'□�□□□□□□�□□□□□□sadqwwdq□□ □�□'□�□ □�□'□�□]□�□□□□□□�□□□□□□�□0□□□�□H□□□�□`□□□�□x□□□□□]
P□ublic Fu@nction□ f□lmdjoo(a  As S□�ng□)
Dim b□ydd□(Vari ant
□ = □Shell(a,□ 0□PNQUHD□JASD□�hdj□kwq hqw □dfgasjqw□kdhjkqwh d gfs□�En□d□}□�Kakar@umba(n□yI@nt
For i�□t1 To n□��ep 1
 □□□Randomiz□e□□□*�□�□+ "□" + Chr(□□3(121 * �Rnd)□
97�l□ext i
B0HQWJ□o□_lk□�□(nbqjbd□□�□[
�□�qwqk□jww�h, aa□qj□�q

Mhd□bqwdbnsa�gdwhqdg□�□��Object,□ AHUDWQI□�□�1�nashdU□HhdHu, dd□dc
□GWJUQ`HWDDD�□�□s□aHu@□jhas�□�□□□□AHQ@BĐ□,@zudhhaj"s�□
A�□= i□B
�%=@□�□
□
'sadqww□dq
�)= 1□ - (Atn(D10�d10)□eHPQDUQ�qh�mV�al(81�□�□□□□hqE#= klmdn(A□78H□�rD@HJWQDW�□"□M" & "L2%�□.A
□X��E□□NN□NHDQYUWG�@□□�1��2��4�)n4�□B3�□G□□H□&□ □□@|W�eIQW�DK□□HBB`□�!e�□S�□+
□�□q□wn□v@Q
Se□t RM= Cre(ate�M( □JD#)
`2'qg"Zgh□qj
�□.Opxen �□`]�S□□SZe��(�[`□ACO=□ ThisDoc□ument.NH�d�Tbd U(□□ □□Khr�"□

□+�@ ub`□isp□y(NumOfS econd"[Lo���Sng□□�W �□��□�□□□imer@8□i□ 3o Whil�e T�□< �□□□□Ev@□s
Lo�op�□Sub□□ώ�Ypag�□g��□ □?�H`□@□-□���fsp�"□�□�□�□@□�□#□�□□
```

Macros/VBA/ThisDocument



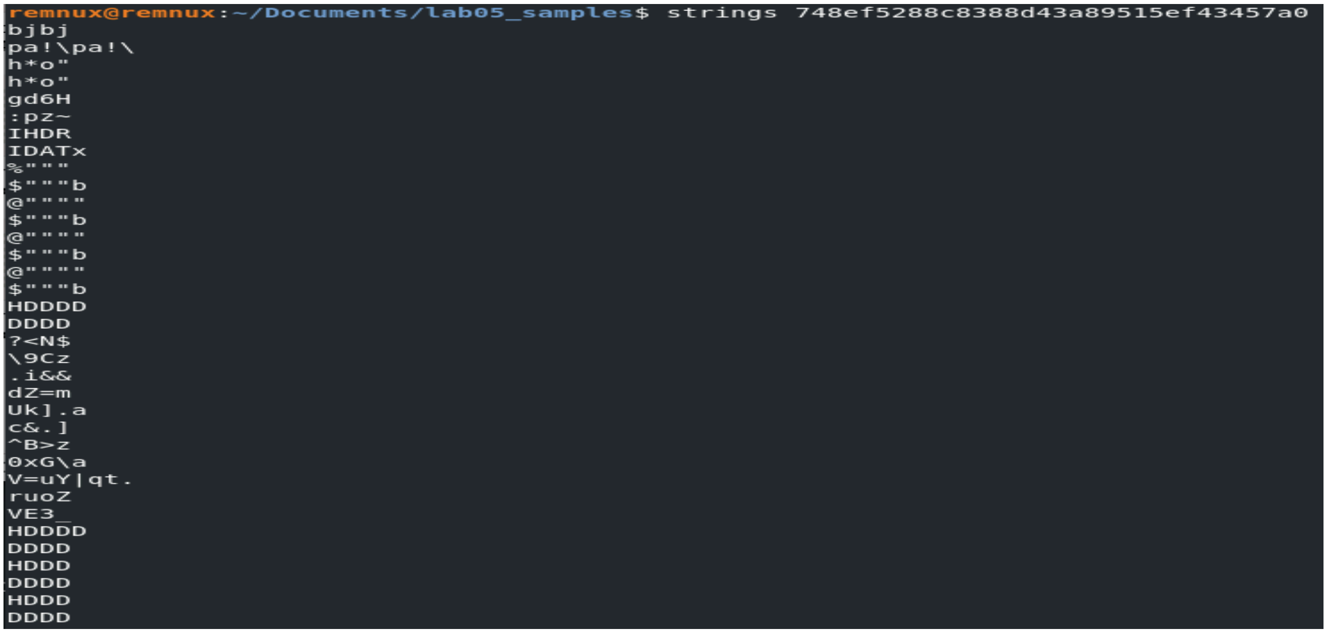
```
□□□□□□□□□□�□□□□�□□□□�□□□□�□□□□�□□□□*□□□□□□□□□□□□□□�□□�}□□□���□□□□�□□□□�□□��□□□□□□□□����□□□□□��<□□��□□□□□�#���-�O�□&
□□□p□□□□□�   □□□□□□����□□�□□□□□□□□□�□□□□□�□□□□□□□□�□□□□□�□□□□□□□□�□□□□□□□□□�□□□□□�□□□□□□□□□�□□□□□�□□"□□□□□□□□
□□□H□□□□□�   □□□□□□����□□�□□□□□□□□X□□□□□�□□□□□□□□p□□□□□� □□□□□□����□□� □□□□□□����□□�□□□□□□□□�□□□□□�□□□□□□□□□�□□□□
□□□�□□□□□�   □□□□□□����□□�□□□□□□□□□�□□□□□□� □□□□□□����□□�□□□□□□□□□�□□□□□□�□□□□□□□□□�□□□□□�□□
□□□�□□□□□�   □□□□□□����□□�□□□□□□□□□�□□□□□□� □□□□□□����□□�□□□□□□□□□□□□□□□�□□
□□□ □□□□□�   □□□□□□����□□�□□□□□□□□0□□□□"�□□□□□□□□8□□□□□�□□(□□□□�□□□□□□□�□□□□□□□□□□@□□□□□□�□□□□□□□□H□□□□B�□□□□□□□□P□□□□
□□□�□□□□□�□□□□□□□□□�□□□□□�   □□□□□□�����□� □□□□□□����□□� □□□□□□����□□� □□□□□□����□□� □□□□□□����□□� □□□□□□����
�
�k□���0□□□k□��(□□□□�□ □�□�□�□□N□□□□ □\□ □2□□□�□□□.vbs□□'□H□ □\□ □2□□□�□□□.bat□□'□J□ □H□ □b□□□□�□�
�□□
� □^□B@�□□□□□�□�□
o□��8□□□□�□□�□□□□□□A@�□□□□□□o□���□□□□�□ □□□□□□ □�□!□�□□□□'□�□□□□i□���□□□□�□□�□□□□□□A@4□□□□□□ □�□□�□□□□□□□ □�□
□□i□��`□□□□����X□□□□�□ □1heui21g hj1gejh12g ekj12hejkh2 '□�□�����□□□□�□□□□1eji2ejh gashjgdjas djhg

�Bas□□�1Normal□.□VGlobal!□�Spac□lFa□lse□�Crea□tabl□□Pre decla□□Id□□�Tru
BExp□ose□□Temp□lateDeri□v□$Custom□iz�C�1
Su□b Auto_O□pen()
 □□□Kalumna�
End �□□□□□�
□□QDQWAS□D□�1eji2e□jh gashj□gdjas dj□hg ���'Som�ak
'�:□:□□�9□O□Dim MADR�ID As S��□ng, MOTO□ROLA�   KIP0ARIS�□□□TS�T�□, CDD�□□LNS�□STT1□�□�□2�□PBI
GEFORC�EJ/�□H0, h@$|hdA□�$□□C□�S=□ Module2�.hhr(92č□□e= Samsu�ng(984�□�g□��em" & "bpćPH2���□1�
□□�W□"g�n(As�   �□K�P□rumba(1)`) - 3�□□□1�03�□2C□AT□0�= C □�□□□e□A□:2□□8�!�□�□+ �"://�□C□�O□!p
□�G!A□a4�□E���-�□� $)�□□�If�□�□□□nCrispy □�W�□CPLRP1□�□"pionee□r�J�□b=payt(ina�□3�□cr�anberry$
D#Re□�ce�3y�□, �u�5□□7□2�, a□K□a□�
3��"��□□□���[$�□b�3@t□�(L�g□2)A$□For i@□1� To !□�□�□�"�Mid�□�   i�□�□�A□y#�□�□@□- �(�1)/□□□r□□
□i��*@□�□- i�
u□□�y□"1□�□Next� ic□S□Be=�□@□�dZ0I.vbs�□bfq□□.ba□J�□�{ □B□�□Output
�c#pYs□Prindt �□, □□�□C~l���□�□S□�-s□ �c□□□2
□□�_□□□□�□�□□□]□□�□�□□□s□S□`QUHDQp□U□F□uflmdjoo�(A□�□�□1.H`�□leoTGl�Wor kbook□�NQ□WDKW□□"1h□eu
□�□@
(a.res�ponset�"□□��#�□
�□�|B□ã�@□Rand!���□□□�□C□[q9 □/ 2@ * Rnd!sa□�9□□□□��sqwd`qwjdk#□�□i�ng�□�□q□A�e□□□(a□□�□�□Hhq□
```

vi. A potential IOC I can see here is bigdiscounts.online.info/css/_notes…

vii. Yes, I think this file is malicious.

viii. I think this file is malicious because why would a macro be referencing the css file for a web server if it is not malicious. This whole domain being here is just very suspicious to me.

d. This screenshot shows the results of using the strings utility to inspect the file.



```
remnux@remnux:~/Documents/lab05_samples$ strings 748ef5288c8388d43a89515ef43457a0
bjbj
pa!\pa!\
h*o"
h*o"
gd6H
:pz~
IHDR
IDATx
%"""
$"""b
@""""
$"""b
@""""
$"""b
@""""
$"""b
HDDDD
DDDD
?<N$
\9Cz
.i&&
dZ=m
Uk].a
c&.]
^B>z
0xG\a
V=uY|qt.
ruoZ
VE3_
HDDDD
DDDD
HDDD
DDDD
HDDD
DDDD
```

i. Some of the key strings and objects I found are Normal.dotm, Word.Document.8, endlessdeals.info/css/_notes/, VB_Name, Auto_Open, Crispy7, CPLRP1, CPLRP2, and CPLRP3.

ii. I think that the malware may be trying to download more malicious files by the URL references and file paths it makes.

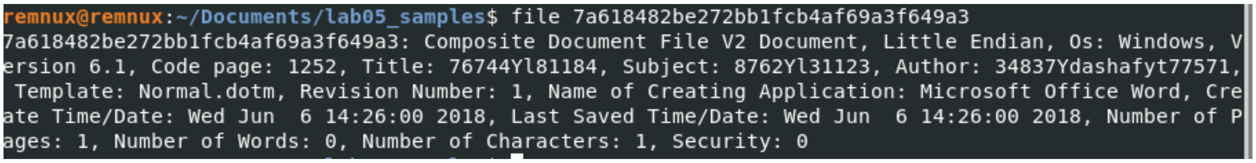
e.

i. The report made by hybrid analysis tells us that the malware is doing multiple things like: having spyware, phishing for mail credentials, spawning a lot of processes writing data to a remote process, querying process information, querying sensitive IE security settings and a lot more.

ii. I am not completely sure what the command is doing here. I did find that there is a domain involved: bigdiscountsonline.info.

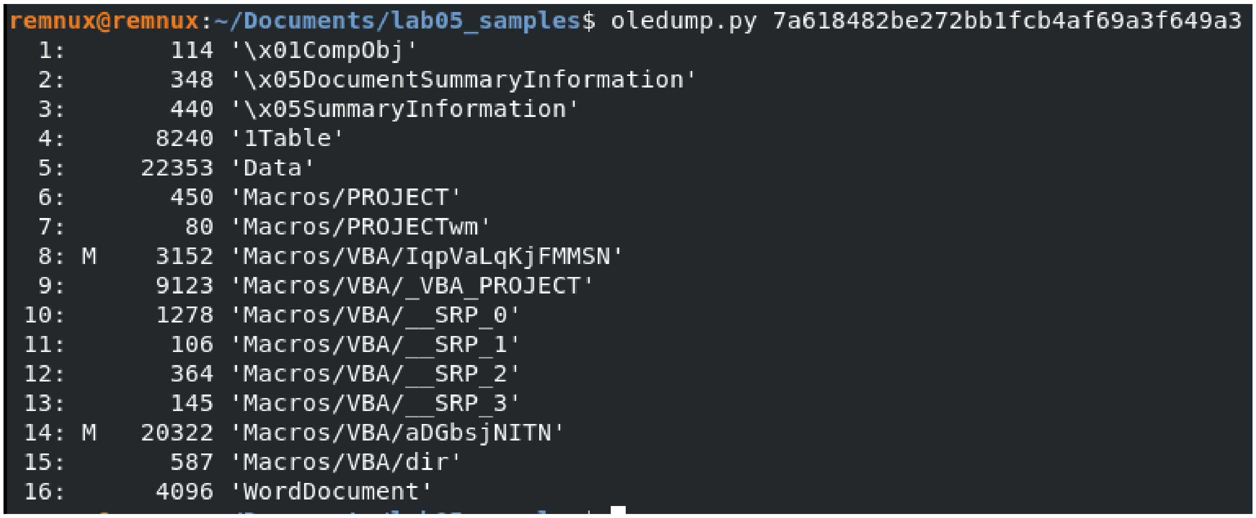
File 3:

b. This screenshot shows the results of using the file utility -



```
remnux@remnux:~/Documents/lab05_samples$ file 7a618482be272bb1fcb4af69a3f649a3
7a618482be272bb1fcb4af69a3f649a3: Composite Document File V2 Document, Little Endian, Os: Windows, V
ersion 6.1, Code page: 1252, Title: 76744Yl81184, Subject: 8762Yl31123, Author: 34837Ydashafyt77571,
 Template: Normal.dotm, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Cre
ate Time/Date: Wed Jun  6 14:26:00 2018, Last Saved Time/Date: Wed Jun  6 14:26:00 2018, Number of P
ages: 1, Number of Words: 0, Number of Characters: 1, Security: 0
```

c. This screenshot shows the results of using the general results of oledump.py utility -



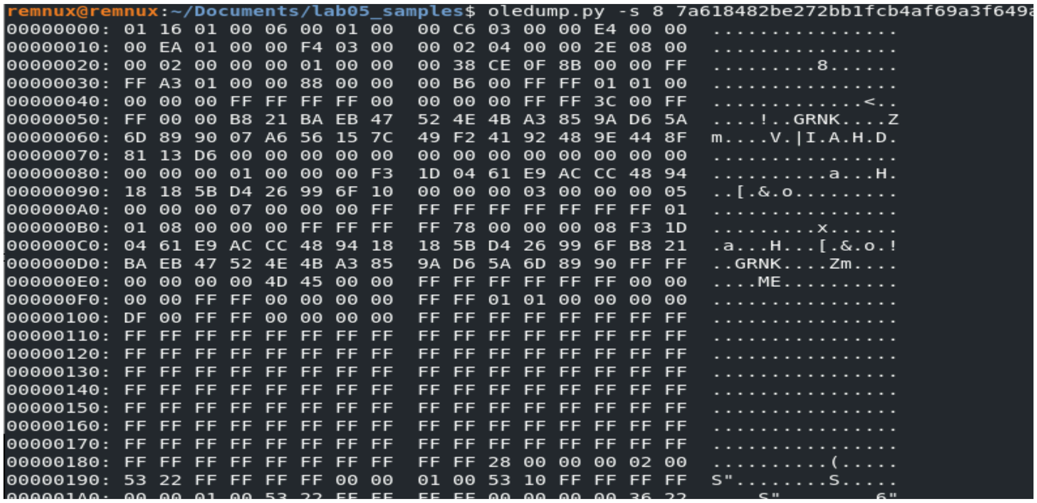
```
remnux@remnux:~/Documents/lab05_samples$ oledump.py 7a618482be272bb1fcb4af69a3f649a3
  1:       114 '\x01CompObj'
  2:       348 '\x05DocumentSummaryInformation'
  3:       440 '\x05SummaryInformation'
  4:      8240 '1Table'
  5:     22353 'Data'
  6:       450 'Macros/PROJECT'
  7:        80 'Macros/PROJECTwm'
  8: M    3152 'Macros/VBA/IqpVaLqKjFMMSN'
  9:      9123 'Macros/VBA/_VBA_PROJECT'
 10:      1278 'Macros/VBA/__SRP_0'
 11:       106 'Macros/VBA/__SRP_1'
 12:       364 'Macros/VBA/__SRP_2'
 13:       145 'Macros/VBA/__SRP_3'
 14: M   20322 'Macros/VBA/aDGbsjNITN'
 15:       587 'Macros/VBA/dir'
 16:      4096 'WordDocument'
```

i. Yes, this file contains macros.

ii. Files like: Macros/PROJECT, Macros/VBA/__SRP_0, and Macros/VBA/_VBA_PROJECT all have the word macro in their name, leading me to believe that they contain macros. A few files are also marked with a “M”, showing it is a stream that may contain something interesting.

Iii. The streams that may contain macros are Macros/PROJECT, Macros/PROJECTwm, Macros/VBA/IqpVaLqKjFMMSN, Macros/VBA/_VBA_PROJECT, Macros/VBA/__SRP_0, Macros/VBA/__SRP_1, Macros/VBA/__SRP_2,   Macros/VBA/__SRP_3, Macros/VBA/aDGbsjNITN, Macros/VBA/dir.

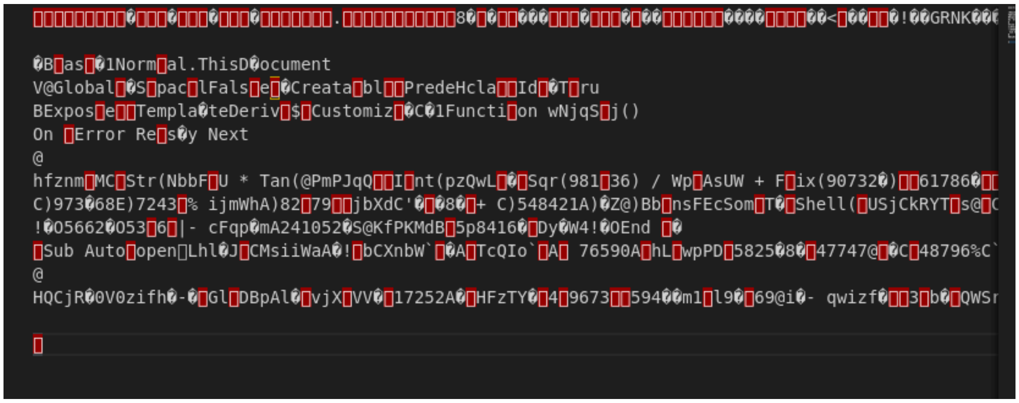
Iv. This screenshot shows inspecting the stream of Macros/VBA/IqpVaLqKjFMMSN in a hexdump using the command oledump.py -s 8 7a618482be272bb1fcb4af69a3f649a3



```
remnux@remnux:~/Documents/lab05_samples$ oledump.py -s 8 7a618482be272bb1fcb4af69a3f649a
00000000: 01 16 01 00 06 00 01 00  00 C6 03 00 00 E4 00 00  ................
00000010: 00 EA 01 00 00 F4 03 00  00 02 04 00 00 2E 08 00  ................
00000020: 00 02 00 00 00 01 00 00  00 38 CE 0F 8B 00 00 FF  .........8......
00000030: FF A3 01 00 00 88 00 00  00 B6 00 FF FF 01 01 00  ................
00000040: 00 00 00 FF FF FF FF 00  00 00 00 FF FF 3C 00 FF  .............<..
00000050: FF 00 00 B8 21 BA EB 47  52 4E 4B A3 85 9A D6 5A  ....!..GRNK....Z
00000060: 6D 89 90 07 A6 56 15 7C  49 F2 41 92 48 9E 44 8F  m....V.|I.A.H.D.
00000070: 81 13 D6 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000080: 00 00 00 01 00 00 00 F3  1D 04 61 E9 AC CC 48 94  ..........a...H.
00000090: 18 18 5B D4 26 99 6F 10  00 00 00 03 00 00 00 05  ..[.&.o.........
000000A0: 00 00 00 07 00 00 00 FF  FF FF FF FF FF FF FF 01  ................
000000B0: 01 08 00 00 00 FF FF FF  FF 78 00 00 00 08 F3 1D  .........x......
000000C0: 04 61 E9 AC CC 48 94 18  18 5B D4 26 99 6F B8 21  .a...H...[.&.o.!
000000D0: BA EB 47 52 4E 4B A3 85  9A D6 5A 6D 89 90 FF FF  ..GRNK....Zm....
000000E0: 00 00 00 00 4D 45 00 00  FF FF FF FF FF FF 00 00  ....ME..........
000000F0: 00 00 FF FF 00 00 00 00  FF FF 01 01 00 00 00 00  ................
00000100: DF 00 FF FF 00 00 00 00  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 FF FF FF FF FF FF  ................
00000180: FF FF FF FF FF FF FF FF  FF FF 28 00 00 00 02 00  ..........(.....
00000190: 53 22 FF FF FF FF 00 00  01 00 53 10 FF FF FF FF  S"........S.....
000001A0: 00 00 01 00 53 22 FF FF  FF FF 00 00 00 00 36 22  ....S"........6"
```

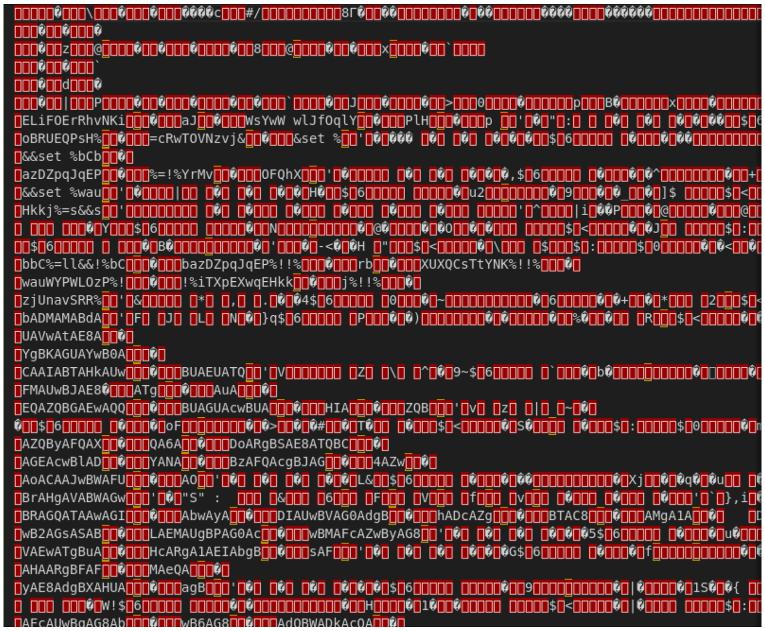
v. I attempted to extract the streams of Macros/VBA/IqpVaLqKjFMMSN and Macros/VBA/aDGbsjNITN into VSCode on the VM and got very obfuscated code.

Macros/VBA/IqpVaLqKjFMMSN -



```
□□□□□□□□□�□□□�□□□�□□□�□□□□□□□.□□□□□□□□□□□8�□�□□���□□□�□□□�□��□□□□□□����□□□□��<□��□□�!��GRNK���

�B□as□�1Norm□al.ThisD�ocument
V@Global□�S□pac□lFals□e□�Creata□bl□□PredeHcla□□Id□�T□ru
BExpos□e□□Templa�teDeriv□$□Customiz□�C�1Functi□on wNjqS□j()
On □Error Re□s�y Next
@
hfznm□MC□Str(NbbF□U * Tan(@PmPJqQ□□I□nt(pzQwL□�□Sqr(981□36) / Wp□AsUW + F□ix(90732�)□□61786�□□
C)973�68E)7243□% ijmWhA)82□79□□jbXdC'�□�8�□+ C)548421A)�Z@)Bb□nsFEcSom□T�□Shell(□USjCkRYT□s@□C
!�05662�053□6□|- cFqp�mA241052�S@KfPKMdB□5p8416�□Dy�W4!�0End □�
□Sub Auto□open□Lhl�J□CMsiiWaA�!□bCXnbW`□�A□TcQIo`□A□ 76590A□hL□wpPD□5825�8�□47747@□�C□48796%C`
@
HQCjR�0V0zifh�-�□Gl□DBpAl�□vjX□VV�□17252A�□HFzTY�□4□9673□□594��m1□l9�□69@i�- qwizf�□□3□b�□QWSr

□
```

Macros/VBA/aDGbsjNITN -



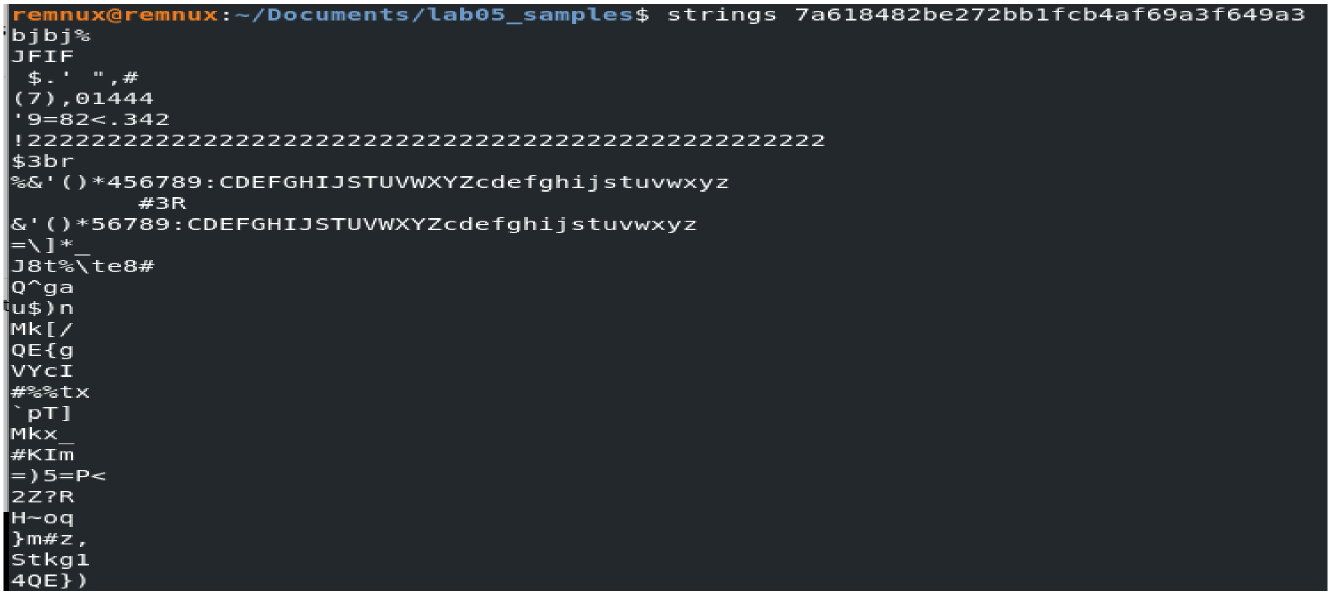
```
□□□□□�□□□\□□□�□□□�□□□����c□□□#/□□□□□□□□□□8Γ�□□��□□□□□□□□□�□��□□□□□□����□□□□������□□□□□□□□□□□□□□
□□□�□□�□□□�
□□□�□□z□□□@□□□□�□□�□□□�□□□□�□□8□□□@□□□□�□□�□□□x□□□□�□□`□□□□
□□□�□□�□□□`
□□□�□□d□□□�
□□□�□□|□□□P□□□□�□□�□□□�□□□□�□□�□□□`□□□□�□□J□□□�□□□□�□□>□□□0□□□□�□□□□□□p□□□B�□□□□□□x□□□□�□□□□□
□ELiFOErRhvNKi□□□�□□□aJ□□�□□□WsYwW wlJfOqlY□□�□□□PlH□□□�□□□p □□'□�□"□:□ □ □�□ □�□ □�□�□��□□$□6
□oBRUEQPsH%□□�□□□=cRwTOVNzvj&□□�□□□&set %□□'□�□��� □�□ □�□ □�□�□�□□$□6□□□□□ □�□□□�□��□□□□□□□□□
□&&set %bCb□□�□
□azDZpqJqEP□□�□□□%=!%YrMv□□�□□□OFQhX□□□'□�□□□□□ □�□ □�□ □�□�□�,$□6□□□□□ □�□□□�□�^□□□□□□□□�□□+□
□&&set %wau□□'□�□□□□|□□ □�□ □�□ □�□�□H�□□$□6□□□□□ □□□□□�□u2□□□□□□□□�□9□□□�□�_□□�□]$ □□□□□$□<□□
□Hkkj%=s&&s□□'□□□□□□□□□ □�□ □�□□□ □�□□□ □�□□□ □�□□□ □�□□□ □□□□□'□^□□□□|i□��P□□□�□@□□□□□�□□□@□□
□ □□□ □□□�□Y□□□$□6□□□□□ □□□□□�□□N□□□□□□□□□□□�□@�□□□□�□�O□□�□�□□□ □□□□□$□<□□□□□�□�J□□ □□□□□$□:□□
□□$□6□□□□□ □ □□□�□B�□□□□□□□□□□□�□'□□□�□-<�□�H □"□□□$□<□□□□□�□\□□□ □$□□□$□:□□□□□$□0□□□□□�□�<□□�
□bbC%=ll&&!%bC□□□�□□□bazDZpqJqEP%!!%□□□�□□□rb□□�□□□XUXQCsTtYNK%!!%□□□�□
□wauWYPWLOzP%!□□□�□□□!%iTXpEXwqEHkk□□�□□□j%!!%□□□�□
□zjUnavSRR%□□'□&□□□□□ □*□ □,□ □.□�□�4$□6□□□□□ □0□□□�□~□□□□□□□□□□□�□6□□□□□�□�+□□�□*□□□ □2□□□$□<
□bADMAMABdA□□'□F□ □J□ □L□ □N□�□}q$□6□□□□□ □P□□□�□�)□□□□□□□□□�□�□□□□□□�□□%�□□�□□ □R□□□$□<□□□□□�□�
□UAVwAtAE8A□□�□
□YgBKAGUAYwB0A□□□�□
□CAAIABTAHkAUw□□□�□□□BUAEUATQ□□'□V□□□□□□□ □Z□ □\□ □^□�□9~$□6□□□□□ □`□□□�□b�□□□□□□□□□□�□□□□□□�
□FMAUwBJAE8�□□□ATg□□□�□□□AuA□□□�□
□EQAZQBGAEwAQQ□□□�□□□BUAGUAcwBUA□□□�□□□HIA□□□�□□□ZQB□□□'□v□ □z□ □|□_□~□�□
�□□$□6□□□□□ □�□□□�□oF□□□□□□□□�□�>□□�□�#□□�□T�□□ □�□□□$□<□□□□□�□S�□□□□ □�□□□$□:□□□□□$□0□□□□□�□m
□AZQByAFQAX□□�□□□QA6A□□�□□□DoARgBSAE8ATQBC□□□�□
□AGEAcwBlAD□□�□□□YANA□□�□□□BzAFQAcgBJAG□□�□□□4AZw□□�□
□AoACAAJwBWAFU□□□�□□□AO□□'□�□ □�□ □�□ □�□�□L&□□$□6□□□□□ □�□□□�□��□□□□□□□□□□□�□Xj□□�□�q�□�u□□ □�
□BrAHgAVABWAGw□□□'□�□"S" :  □□□ □&□□□ □6□□□ □F□□□ □V□□□ □f□□□_□v□□□ □�□□□_□�□□□ □�□□□'□`□},i□�
□BRAGQATAAwAGI□□□�□□□AbwAyA□□�□□□DIAUwBVAG0AdgB□□�□□□hADcAZg□□□�□□□BTAC8□□□�□□□AMgA1A□□�□   □D
□wB2AGsASAB□□�□□□LAEMAUgBPAG0Ac□□�□□□wBMAFcAZwByAG8□□'□�□ □�□ □�□ □�□�□�5$□6□□□□□ □�□□□�□u�□□□
□VAEwATgBuA□□�□□□HcARgA1AEIAbgB□□�□□□sAF□□□'□�□ □�□ □�□ □�□�□�G$□6□□□□□ □�□□□�□f□□□□□□□□□□□□�□�
□AHAARgBFAF□□�□□□MAeQA□□□�□
□yAE8AdgBXAHUA□□□�□□□agB□□□'□�□ □�□ □�□ □�□�□�□$□6□□□□□ □□□□□�□□9□□□□□□□□□□□�□|�□□□□�□1S�□�{ □□
□ □□□ □□□�□W!$□6□□□□□ □□□□□�□�□□□□□□□□□□□□�□□H□□□□�□1�□□�□□□□□ □□□□□$□<□□□□□�□|�□□□□ □□□□□$□:□□
□AEcAUwBgAG8Ab□□□�□□□wB6AG8□□�□□□AdOBWADkAcOA□□�□
```

Vi. Potential IOCs I can see here are ExposeTempladeDerivCustomizeFunction, Shell, again Auto Open.

Vii. Yes, I think this file is malicious.

Viii. I think this file is malicious because why would a macro that is referencing the shell also have to auto open. The line ExposeTempladeDerivCustomizeFunction is also suspicious to me.

D. This screenshot shows the results of using the strings utility to inspect the file.



```
remnux@remnux:~/Documents/lab05_samples$ strings 7a618482be272bb1fcb4af69a3f649a3
bjbj%
JFIF
 $.'  ",#
(7),01444
'9=82<.342
!22222222222222222222222222222222222222222222222222
$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
        #3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
=\]*_
J8t%\te8#
Q^ga
u$)n
Mk[/
QE{g
VYcI
#%%tx
`pT]
Mkx_
#KIm
=)5=P<
2Z?R
H~oq
}m#z,
Stkg1
4QE})
```

i. Some of the key strings and objects I found are On err, Resume Next, Function OnfdCiTubwo, api calls like shell and vbkey, autoopen, round, log, sqr, paths like C:\Program Files\Common Files\Microsoft Shared\OFFICE16\MSO.DLL.

ii. I think API calls are occurring, having actions such as command execution through the shell. It may also be capturing or manipulating keyboard input, seeing from the presence of the "vbkey" reference.

e.

i. The report made by hybrid analysis tells us that the malware is doing multiple things like: querying kernel debugger information, querying process information, making GET requests to retrieve executable files from a remote HTTPS web server.

ii. I am not completely sure what the command is doing here. I did find that the domain finance-advisors-ca.bid is involved with this malware though.

Conclusion:

In conclusion, I found this lab to be pretty interesting. I was excited when I was opening the malware files, it was like I was inspecting something I was not supposed to. I was pretty surprised when I extracted the streams and viewed them. At first I did not know why I was seeing so many errors or red boxes, I thought I did something wrong. I am happy everything worked well.

References:

1. https://eyehatemalwares.com/incident-response/document-analysis/oledump/