

Malware Obfuscation

The Art of Hiding Malware

François Thibaut de Maisières | July 2022

Process of obscuring (hiding/masking)
meaningful information

```
...skipped..
```

```
IPC["ap"+(64>10?"\x70":"\x6a")+"endChi"+l+(67>0?"\x64":"\x5e")+""](document["create"+(72>5?"\x54":"\x4c")+"e"+"xtN"+(70>13?"\x6f":"\x68")+"de"])(hkC+Ypw));;
IPC=IPC["innerH"+(78>47?"\x54":"\x4e")+""+""+(80>32?"\x4d":"\x45")+"L"];;IPC=IPC[""+"repla"+(87>28?"\x63":"\x5a")+"e"](/[\s+\.\/,]/g,"");;
yFS="2d2p1z362e0w2o0x2y2529122h391i2t16363b3d3b1d2a";
for(var vgo=(0*"E\x82G_X0<\x8a;D6\x60^%i-Z["charCodeAt"])(6)+0.0);vgo<IPC["leng"+String.fromCharCode(116)+""+"h"];vgo+=(0*"mIe9;-*H%4h:["charCodeAt"])(7)+2.0)){zE9+=String["from"+(54>40?"\x43":"\x3d")+"h"+"arC"+(62>10?"\x6f":"\x66")+"de"])(parseInt(IPC["su"+(60>39?"\x62":"\x5c")+""+""+(87>35?"\x73":"\x69")+"tr"])(vgo,(0*"xp\x82Jf+l:["length"])+2.0)),a78));;
qB8="x1x362q2t352r2d2w1j2t312r1z302z2d3";;
TlU["toS"+(65>7?"\x74":"\x6b")+"ri"+""+(69>17?"\x6e":"\x67")+"g"]=DuF[""+"constru"+String.fromCharCode(99)+""+"tor"])(zE9);;
yFS="2d2p1z362e0w2o0x2y2529122h391i2t16363b3d3b1d2a";;
zE9=TlU+"2i0y2j1 41k1g1a1c170y162h2p1h2k3c1k1d2";;
hl2="0y2l141b2j2e282b2u2s1z2f, 1d291l2h1c2l1b2v";;
IPC[""+"innerHT"+(90>2?"\x4d":"\x48")+"L"]="0y362t34302p2r2t0y2l141b2j1v2k2n2p322k";;};})();
```


But why obfuscate?

Avoid anti-virus detection

But why obfuscate?

More difficult for analysis

Packing

Encrypt, Compress, Transforme a program


The program is no longer instructions... but data

Being invisible to anti-malware software

Dead-Code Insertion

Inserting some code in the program... That does nothing 🤩

Instruction Substitution

Changes an original code by replacing some instructions with other equivalent ones. 

Base64 Encoding

o3R="ZWNobyAiSSB3YXMgYSBoaWRkZW4gY29tbWFuZCI="

Subrouting Reordering

The subroutines of a programme changes in a random way

Changing the hash of the file

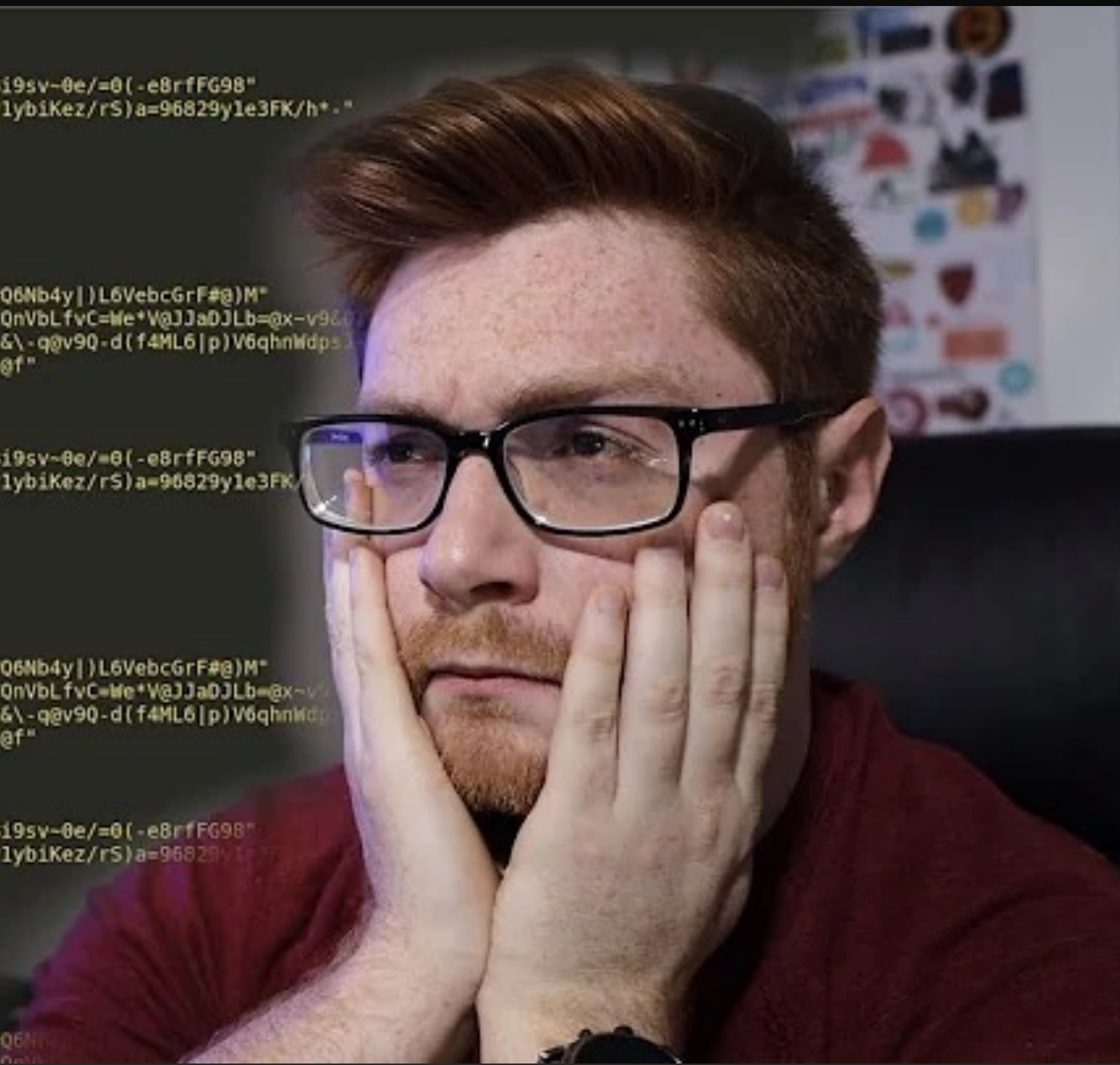
Other techniques

- Pattern/Flow Transformation
- Exclusive OR (XOR)
- ROT13 encoding
- Anti-tamper
- Anti-Debug
- And many more (creativity is your own limite)

```

24632 Function LfLbJdq()
24633 Dim wzWcoSzp,tzaboFcc,sdBHoLsz
24634 Dim i
24635 wzWcoSzp = "wM6)J-/w|K=zGFxFxNDBMrW7i4sBp0ry-xXp6-ipBi9sv-0e/=0(-e8rfF698"
24636 tzaboFcc = "WKJq-/7#zGo0n0z-MX)h-ft2BH0JoFq7nF6-rvFrrlybiKez/rs)a=96829y1e3FK/h+."
24637 If wzWcoSzp <> tzaboFcc Then
24638   sdBHoLsz = wzWcoSzp & tzaboFcc
24639 End If
24640 For i = 1 To 7
24641   LfLbJdq = LfLbJdq & sdBHoLsz
24642 Next
24643 End Function
24644 MWSCLs = "q9=gpMHun*SLqdv@X7v-9p@7N-)z(NpJd0+*qbH|-#Q6Nb4y|)L6VebcGrF#@)M"
24645 GrGJdtMSy = "**+FQnyJSt8yi8yu3H-\)pX&C-M)D4BMhcQF&XgDCQnVbLfvC=Me*V@JJa0JLb=@x-v9&0"
24646 HJCeheH = "NtV0*6=|0ufscW@B\B8ScrdhwKNV4wCFcJJb=(+0-a6\-.q@v9Q-d(f4ML6|p)V6qhnWdps"
24647 SxSzsXoH = "(n#K3FGg4L*0(Bgv12nh=&H-C-d@Ji#o=FCwJK=-hgf"
24648 Function LfLbJdq()
24649 Dim wzWcoSzp,tzaboFcc,sdBHoLsz
24650 Dim i
24651 wzWcoSzp = "wM6)J-/w|K=zGFxFxNDBMrW7i4sBp0ry-xXp6-ipBi9sv-0e/=0(-e8rfF698"
24652 tzaboFcc = "WKJq-/7#zGo0n0z-MX)h-ft2BH0JoFq7nF6-rvFrrlybiKez/rs)a=96829y1e3FK/h+."
24653 If wzWcoSzp <> tzaboFcc Then
24654   sdBHoLsz = wzWcoSzp & tzaboFcc
24655 End If
24656 For i = 1 To 7
24657   LfLbJdq = LfLbJdq & sdBHoLsz
24658 Next
24659 End Function
24660 MWSCLs = "q9=gpMHun*SLqdv@X7v-9p@7N-)z(NpJd0+*qbH|-#Q6Nb4y|)L6VebcGrF#@)M"
24661 GrGJdtMSy = "**+FQnyJSt8yi8yu3H-\)pX&C-M)D4BMhcQF&XgDCQnVbLfvC=Me*V@JJa0JLb=@x-v9&0"
24662 HJCeheH = "NtV0*6=|0ufscW@B\B8ScrdhwKNV4wCFcJJb=(+0-a6\-.q@v9Q-d(f4ML6|p)V6qhnWdps"
24663 SxSzsXoH = "(n#K3FGg4L*0(Bgv12nh=&H-C-d@Ji#o=FCwJK=-hgf"
24664 Function LfLbJdq()
24665 Dim wzWcoSzp,tzaboFcc,sdBHoLsz
24666 Dim i
24667 wzWcoSzp = "wM6)J-/w|K=zGFxFxNDBMrW7i4sBp0ry-xXp6-ipBi9sv-0e/=0(-e8rfF698"
24668 tzaboFcc = "WKJq-/7#zGo0n0z-MX)h-ft2BH0JoFq7nF6-rvFrrlybiKez/rs)a=96829y1e3FK/h+."
24669 If wzWcoSzp <> tzaboFcc Then
24670   sdBHoLsz = wzWcoSzp & tzaboFcc
24671 End If
24672 For i = 1 To 7
24673   LfLbJdq = LfLbJdq & sdBHoLsz
24674 Next
24675 End Function
24676 MWSCLs = "q9=gpMHun*SLqdv@X7v-9p@7N-)z(NpJd0+*qbH|-#Q6Nb4y|)L6VebcGrF#@)M"
24677 GrGJdtMSy = "**+FQnyJSt8yi8yu3H-\)pX&C-M)D4BMhcQF&XgDCQnVbLfvC=Me*V@JJa0JLb=@x-v9&0"

```



MALWARE ANALYSIS - VBScript Decoding & Deobfuscating

THANK YOU