

ウイルス解析報告書

ウイルス名	W32.Bugbear.B@mm (別名: Win32.Bugbear.B [CA], W32/Bugbear.b@MM [McAfee], PE_BUGBEAR.B [Trend], W32/Bugbear-B [Sophos], I-Worm.Tanatos.b [KAV], W32/Bugbear.B [Panda], Win32/Bugbear.B@mm [RAV])
プログラム名及び容量(添付ファイル名)	プログラム名: 英文字からなるファイル名で拡張子が exe(感染コンピュータにコピーされるワームの実体) 容 量: 72,192 バイト 添付ファイル名: 「ウイルス動作概要」内参照
種 別	ワーム、ウイルス
プログラム言語	Microsoft Visual C++
発 症 環 境	Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me
発 見 日 時	2003 年 6 月 6 日
発見場所(発信地)	オーストラリア(最初の感染報告があった場所)
危 険 性	大量にメールを送信するだけでなくネットワーク共有を介しても感染を広げる。感染力が強く、短時間に多くの届出が寄せられた。また、一旦感染してしまうとバックドアが仕掛けられたり、キーロガーが仕掛けられたりするため、個人情報が盗み出されてしまう可能性もあり非常に危険である。危険度は 5 段階の 4
発 症 条 件	「不適切な MIME ヘッダーが原因で Internet Explorer が電子メールの添付ファイルを実行する (MS01-020)」という脆弱性問題が解消されていないコンピュータ上で、メールを開いたとき、あるいはメールをプレビューしたときに感染する。または添付ファイルを開いたとき感染する。
ウイルスの活動、影響	感染したコンピュータの特定のファイルからメールアドレスを収集し、全てのアドレスに対し独自の SMTP エンジンを使用し自分自身を送信する大量メール送信ワームで、ネットワーク共有を介しても感染を広げる。 事前に定義済みのリストにある実行形式ファイルにも感染する。ポリモーフィック(変異型)。 キーストロークのログ生成機能やバックドア機能も持っている。様々なウイルス対策プログラムやファイアウォールプログラムのプロセスを停止させようとする。
被 害 規 模	大規模(2003 年 6 月 11 日までに 18173 件(国内は 155 件)の届出がシマンテックに寄せられている)
変種、亜種の有無	W32.Bugbear@mm(2002 年 9 月 30 日発見)の亜種で、発病症状に異なる点がみられる。
ウイルスの動作概要	ウイルスによって送信されるメールには以下の特徴がある。 件名: <ul style="list-style-type: none"> ・ Hello! ・ update ・ hmm.. ・ Payment notices ・ Just a reminder ・ Correction of errors ・ history screen ・ Announcement ・ Various ・ Introduction ・ Interesting... ・ I need help about script!!! ・ Stats ・ Please Help... ・ Report ・ Membership Confirmation ・ Get a FREE gift! ・ Today Only

- New Contests
- Lost & Found
- bad news
- wow!
- Fantastic
- click on this!
- Market Update Report
- empty account
- My eBay ads
- Cows
- 25 merchants and rising
- CALL FOR INFORMATION!
- new reading
- Sponsors needed
- SCAM alert!!!
- Warning!
- its easy
- free shipping!
- News
- Daily Email Reminder
- Tools For Your Online Business
- New bonus in your cash account
- Your Gift
- Re:
- \$150 FREE Bonus!
- Your News Alert
- Hi!
- Get 8 FREE issues - no risk!
- Greetings!

本文 : 無し

添付ファイル名 :

ウイルスに感染したコンピュータの MyDocuments フォルダ内に保存されてファイル名を使用する場合と以下の文字列と拡張子を組み合わせてたファイル名を使用する場合がある。

ファイル名として使用される文字列

- readme
- Setup
- Card
- Docs
- news
- image
- images
- pics
- resume
- photo
- video
- music
- song
- data

ファイル名に使用される拡張子

- ・ .reg
- ・ .bat
- ・ .diz
- ・ .txt
- ・ .cpp
- ・ .html
- ・ .htm
- ・ .jpeg
- ・ .jpg
- ・ .gif
- ・ .cpl

添付ファイル名は、使用されるファイル名に以下の拡張子を付け加え、2重拡張子となる。

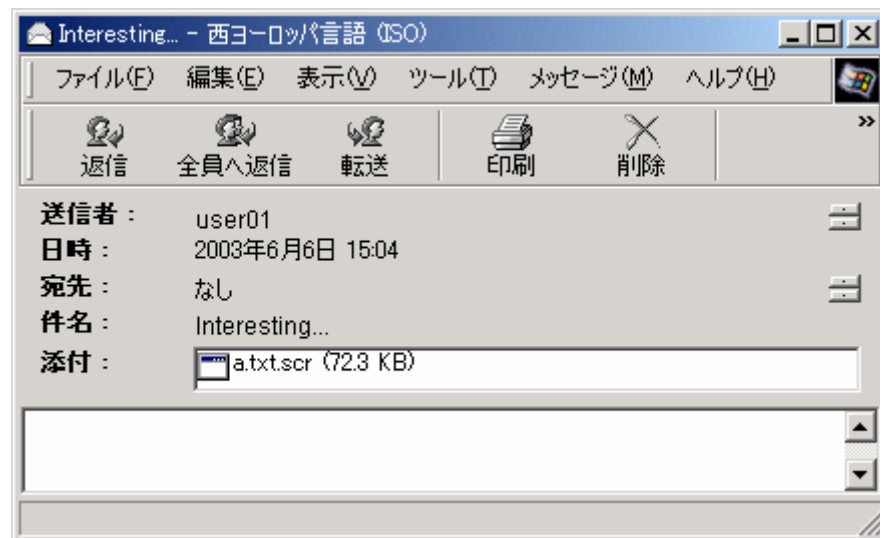
- ・ exe
- ・ pif
- ・ scr

拡張子は乱数で決定され、選択される確立は「scr」が2分の1、「exe」、「pif」が4分の1ずつである。

メッセージのコンテンツタイプは、ファイル名として使用されるファイルタイプと一致し、以下のいずれかになる。

- ・ image/gif
- ・ image/jpg
- ・ text/html
- ・ text/plain
- ・ application/octet-stream

送信されるメールの例

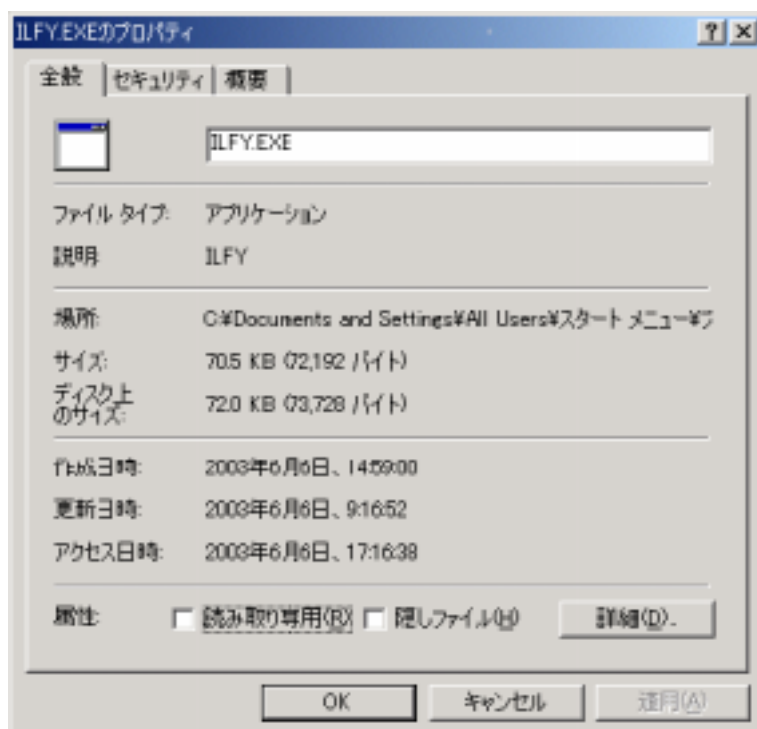


W32.Bugbear.B@mm が実行されると次の動作を行う。

1. Windows のスタートアップフォルダ (Windows 95/98/Me の場合: C:\Windows\Allusers\スタートメニュー\プログラム\スタートアップ。また、WindowsNT/2000/XP の場合: C:\Documents and Settings\<ユーザー名>\スタートメニュー\プログラム\スタートアップ) に自分自身をコピーする。

ファイル名は、XXXX.exe (X はランダムな英文字) となる。

参考: スタートアップにファイル名 ILFY.EXE として蔵置されたワームの実行ファイル。



2. ウィルスは、以下の拡張子等をもつファイルからメールアドレスを収集する。

- ・ INBOX
- ・ .dbx
- ・ .tbb
- ・ .eml
- ・ .mbx
- ・ .nch
- ・ .mmf
- ・ .ods

3. 現在のユーザのメールアドレス及び SMTP サーバを次のレジストリキーから取り出す。

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Account Manager\Accounts

4. 収集した全てのメールアドレスに対し、ウィルス自身が持つ SMTP エンジンを使用してメールを送信する。差出人は、収集したメールアドレスを使用するかレジストリキーから取り出したメールアドレスを使用し詐称される。

ただし、収集したメールアドレスの中に以下の文字列が含まれている場合は、メールを送信しない。

- ・ remove

- spam
- undisclosed
- recipients
- noreply
- lyris
- virus
- trojan
- mailer-daemon
- postmaster@
- root@
- nobody@
- localhost
- localdomain
- list
- talk
- ticket
- majordom

5. ローカル及びネットワーク上にある、次のファイル名に一致するファイルにも感染し、感染の際、このワームはファイルの最後尾に自分自身を追加して変異させる。

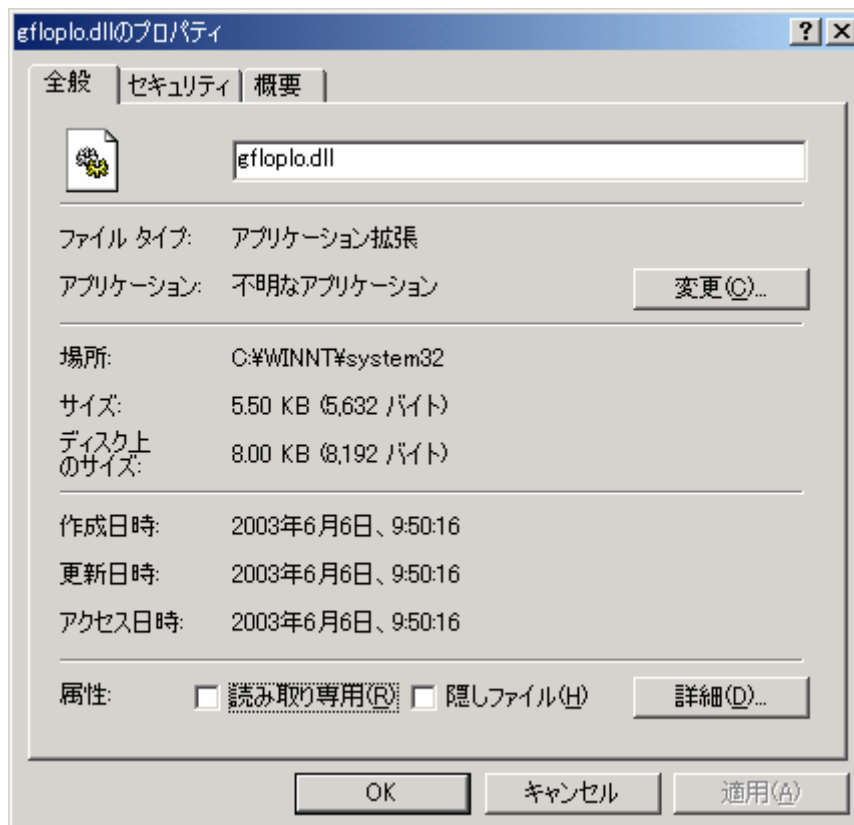
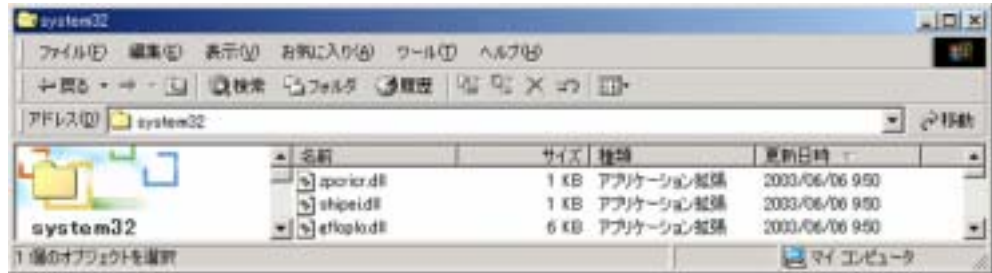
- scandskw.exe
- regedit.exe
- mplayer.exe
- hh.exe
- notepad.exe
- winhelp.exe
- Internet Explorer¥iexplore.exe
- adobe¥acrobat 5.0¥reader¥acrord32.exe
- WinRAR¥WinRAR.exe
- Windows Media Player¥mplayer2.exe
- Real¥RealPlayer¥realplay.exe
- Outlook Express¥msimn.exe
- Far¥Far.exe
- CuteFTP¥cutftp32.exe
- Adobe¥Acrobat 4.0¥Reader¥AcroRd32.exe
- ACDSee32¥ACDSee32.exe
- MSN Messenger¥msnmsgr.exe
- WS_FTP¥WS_FTP95.exe
- QuickTime¥QuickTimePlayer.exe
- StreamCast¥Morpheus¥Morpheus.exe
- Zone Labs¥ZoneAlarm¥ZoneAlarm.exe
- Trillian¥Trillian.exe
- Lavasoft¥Ad-aware 6¥Ad-aware.exe
- AIM95¥aim.exe
- Winamp¥winamp.exe
- DAP¥DAP.exe
- ICQ¥Icq.exe
- kazaal¥kazaal.exe
- winzip¥winzip32.exe

6. ネットワーク共有資源への感染活動に際し、全ての共有ネットワーク上のコンピュータに対し、自分自身をコピーしようとする。さらに、自分自身をそれらのコンピュータの Windows Startup フォルダにコピーしようとする。

ウィルスは、コンピュータとプリンタの区別をしないため、自分自身を誤ってプリントジョブとして追加してしまい、結果的に共有プリンタが正常に動作しなくなる恐れがある。

7. キーログ生成プログラムを、システムフォルダ%System%(標準では、Windows95/98/Me の場合: C:\Windows\System%, WindowsNT/2000 の場合: C:\WINNT\System32%, WindowsXP の場合: C:\Windows\System32%)にランダムな名前の DLL ファイル(サイズは 5632 バイト)を作成する。

参考: ワームによって作成されたキーログ生成プログラム gflplo.dll



8. キーログ生成プログラムにより暗号化されたファイルを Windows フォルダ(標準では C:\Windows または C:\WINNT) 及びシステムフォルダ%System%作成する。この暗号化されたファイルの名前はランダムで拡張子は、DLL 又は DAT のいずれかであり、その中にはキーストロークのデータや構成情報が格納される。また、最前面に表示されているウィンドウ内のテキスト及びクリップボード上にあるデータのログを作成する。

これらのキーログ情報等は、2 時間毎又はファイルサイズが 25,000 バイトを超えたときに、以下のいずれかのメールアドレスに送信される。

・ WXUdeba@mail.com.fr

- ・ beamhardca@11.com
- ・ glucarini@email.it
- ・ sohailam@brain.com.pk
- ・ tiharco@mail.gr
- ・ tjtoll@arabia.com
- ・ lilmoore2@lycos.com
- ・ oktemh@excite.com
- ・ tdawn@hawaiiicity.com
- ・ raytje167@freemail.nl
- ・ ernstdor@online.ie
- ・ mbednar@emailpinoy.com
- ・ marko.aid.001@mail.com
- ・ ellekot@freemail.lt
- ・ bleon@personal.ro
- ・ jackk@biwemail.com
- ・ newhot@mail.az
- ・ joterj@katamail.com
- ・ ektsr@ureach.com
- ・ wejzc@student.be
- ・ rfewr@afreeinternet.com
- ・ wqsg@ashelville.com
- ・ john3784@catholic.org
- ・ iyut@dcemail.com
- ・ asgsa@thedoghousemail.com

キーログ情報を送信する際、まずレジストリを設定を変更して自動ダイヤルの機能を無効にする。キーログ情報の送信が完了すると自動ダイヤルの設定を元に戻す。

9. 世界中の多数の金融機関のドメイン名収録(1376件が確認されている)したリストを保有している。感染したコンピュータのデフォルトのメールアドレスが、リストの中にあるドメイン名と一致した場合、キャッシュ情報に保存されているダイヤルアップ・ネットワーク接続パスワードの情報とともにキーログ情報等が2時間毎又はファイルサイズが25,000バイトを超えたときに、以下のいずれかのメールアドレスに送信される。

- ・ ifrbr@canada.com
- ・ sdorad@juno.com
- ・ fbnfgh@email.ro
- ・ eruir@hotpop.com
- ・ ersdes@truthmail.com
- ・ eofb2@blazemail.com
- ・ ioter5@yook.de
- ・ iuery@myrealbox.com
- ・ jkfhw@wildemail.com
- ・ ds2iahf@kukamail.com

10. 特定のセキュリティ製品のプロセスを停止しようとする。リストに記載された対象となるプロセスは以下のとおりである。

- ・ ZONEALARM.EXE
- ・ WFINDV32.EXE
- ・ WEBSCANX.EXE
- ・ VSSTAT.EXE

- VSHWIN32.EXE
- VSECOMR.EXE
- VSCAN40.EXE
- VETTRAY.EXE
- VET95.EXE
- TDS2-NT.EXE
- TDS2-98.EXE
- TCA.EXE
- TBSCAN.EXE
- SWEEP95.EXE
- SPHINX.EXE
- SMC.EXE
- SERV95.EXE
- SCRSCAN.EXE
- SCANPM.EXE
- SCAN95.EXE
- SCAN32.EXE
- SAFEWEB.EXE
- RESCUE.EXE
- RAV7WIN.EXE
- RAV7.EXE
- PERSFW.EXE
- PCFWALLICON.EXE
- PCCWIN98.EXE
- PAVW.EXE
- PAVSCHED.EXE
- PAVCL.EXE
- PADMIN.EOUTPOST.EXE
- NVC95.EXE
- NUPGRADE.EXE
- NORMIST.EXE
- NMAIN.EXE
- NISUM.EXE
- NAVWNT.EXE
- NAVW32.EXE
- NAVNT.EXE
- NAVLU32.EXE
- NAVAPW32.EXE
- N32SCANW.EXE
- MPFTRAY.EXE
- MOOLIVE.EXE
- LUALLEXE
- LOOKOUT.EXE
- LOCKDOWN2000.EXE
- JEDI.EXE
- IOMON98.EXE
- IFACE.EXE
- ICSUPPNT.EXE
- ICSUPP95.EXE

- ICMON.EXE
- ICLOADNT.EXE
- ICLOAD95.EXE
- IBMAVSP.EXE
- IBMASN.EXE
- IAMSERV.EXE
- IAMAPP.EXE
- FRW.EXE
- FPROT.EXE
- FP-WIN.EXE
- FINDVIRU.EXE
- F-STOPW.EXE
- F-PROT95.EXE
- F-PROT.EXE
- F-AGNT95.EXE
- ESPWATCH.EXE
- ESAFE.EXE
- ECENGINE.EXE
- DVP95_0.EXE
- DVP95.EXE
- CLEANER3.EXE
- CLEANER.EXE
- CLAW95CF.EXE
- CLAW95.EXE
- CFINET32.EXE
- CFINET.EXE
- CFIAUDIT.EXE
- CFIADMIN.EXE
- BLACKICE.EXE
- BLACKD.EXE
- AVWUPD32.EXE
- AVWIN95.EXE
- AVSCHED32.EXE
- AVPUPD.EXE
- AVPTC32.EXE
- AVPM.EXE
- AVPDOS32.EXE
- AVPCC.EXE
- AVP32.EXE
- AVP.EXE
- AVNT.EXE
- AVKSERV.EXE
- AVGCTRL.EXE
- AVE32.EXE
- AVCONSOLE.EXE
- AUTODOWN.EXE
- APVXDWIN.EXE
- ANTI-TROJAN.EXE
- ACKWIN32.EXE

	<ul style="list-style-type: none"> ・ _AVPM.EXE ・ _AVPCC.EXE ・ _AVP32.EXE <p>11. バックドアとして port1080 を開き、攻撃者が感染コンピュータを遠隔で操作可能にする。</p> <ul style="list-style-type: none"> ・ 攻撃者が遠隔から接続してセッションを確立させるために必要な Session Key が書き込まれたファイル及び Serial Number(各システム固有の数値 9 桁)を含むシステムに関する情報を収集したファイルをテンポラリフォルダ(標準では、Windows95/98/Me の場合: C:\Windows\Temp、WindowsNT/2000/XP の場合: %Documents and Settings%ユーザー名\Local Setting\Temp)に作成する。ファイル名はランダムであり、拡張子は.tmp となる。Session Key は、アルファベットと数字からなる 20 文字のデータファイルである。 ・ Session Key を取得した攻撃者は、そのキーを使用し特定のコマンドを入力することでバックドアからウイルスに感染したコンピュータへ侵入し、以下のようなコマンドが実行される可能である。 <ul style="list-style-type: none"> ・ ファイルのコピー ・ ファイルの削除 ・ ファイルの検索 ・ Web ブラウザからファイル一覧情報の取得 ・ コンピュータのシステム情報の取得 ・ 起動中のプロセス情報の取得 ・ ファイルの実行 等 ・ 収集されるシステムに関する情報は、以下のとおり <ul style="list-style-type: none"> ・ ユーザ: <ユーザ名> ・ プロセッサ: <使用されているプロセッサの種類> ・ Windows バージョン: <Windows のバージョン、ビルド番号> ・ メモリ情報: <使用可能なメモリサイズなど> ・ ローカルドライブとそのタイプ (固定/リムーバブル/RAM ディスク/CD-ROM/リモート等), およびその物理的な特徴 ・ 攻撃者は、感染したコンピュータに対しコマンドを実行することでキーストロークのログや収集された各種情報を取得することが可能である。
感染・発症防止方法	<ol style="list-style-type: none"> 1. このワームは、「不適切な MIME ヘッダーが原因で Internet Explorer が電子メールの添付ファイルを実行する(MS01-020)」という脆弱性を利用し、パッチが未適用のシステム上でメールを読んだりプレビューしたりするだけで添付されてあるワームが自動的に実行されるようにしている。対策としては、以下のサイトから適切な修正プログラムを適用する必要がある。 http://www.microsoft.com/japan/technet/security/bulletin/ms01-020.asp 2. 予期せぬメールが届いた場合には、安易にメールを開封しない。特に「ウイルスの動作概要」に記述した内容のメールには注意する。また、.scr、.pif、.exe の拡張子が付いた添付ファイルは安易に開かない。 3. 不要なネットワーク共有を切断する。 4. ネットワーク共有する場合にはパスワードを設定し容易にアクセスできないようにする。
ウイルスの駆除方法	<p>感染コンピュータにコピーされるワームの実体のファイル名がランダムに生成されるため特定が困難であり、またローカル及びネットワーク上にある一般的に使用される実行ファイルにも感染するため、駆除ツール等を使わず手で駆除するのは困難である。</p> <p>無償修復ツールがワクチンベンダーから配布されているので、使用上の注意をよく読み自己責任において使用すること。</p>
その他	なし