

ウイルス解析報告書

ウイルス名	W32.Beagle.AV@mm (別名 : Win32.Bagle.AQ [Computer Associates], Bagle.BC [Panda], WORM_BAGLE.AT [Trend Micro], Bagle.AT [F-Secure], W32/Bagle.AQ@mm [Norman], W32/Bagle.bb@mm [McAfee], W32/Bagle-AU [Sophos])
プログラム名及び容量 (添付ファイル名)	プログラム名 : 不定 容 量 : 不定
種別	ワーム
プログラム言語	C
発症環境	Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP
発見日時	2004 年 10 月 28 日 23:59 (米国太平洋標準時), 2004 年 10 月 29 日 15:39 (日本時間)
発見場所	日本 (最初の感染報告)
危険性	感染力が強い。危険度は 5 段階の 3 (5 が最も危険)。
発症条件	ワームによって作成されたメールの添付ファイルを実行したとき。
ウイルスの活動、影響	このワームは、独自の SMTP エンジンおよびファイル共有ネットワークを利用して拡散を試みる大量メール送信型のワームである。また、感染したコンピュータ上に TCP ポート 81 でバックドアを開く。
被害の規模	発見から 5 時間で 257 件の届出がシマンテック社に寄せられている。
亜種、変種の有無	W32.Beagle@mm
ウイルスの動作概要	<p>ワームにより送信されるメールには次の特徴がある。</p> <p>送信者: 差出人アドレスは詐称されている。</p> <p>件名: 次のうちのいずれかを使用する。 Re: Re: Hello Re: Hi Re: Thank you! Re: Thanks :)</p> <p>本文: :))</p> <p>添付ファイル: ファイル名は、次のうちのいずれかを使用する。拡張子は、.com, .cpl, .exe, または .scr が付く Price price Joke</p> <p>ワーム が実行されると、次のことを行う</p> <p>1. 自分自身のコピーを作成する。 %System%¥wingo.exe %System%¥wingo.exeopen %System%¥wingo.exeopenopen</p> <p>また、他にも自分自身をコピーする可能性がある。 %System%¥wingo.exeopenopenopen</p>

%System%\%wingo.exeopenopenopenopen

Windows のシステムフォルダ%System% (標準では、C:\Windows\system、C:\WINNT\system32 または C:\Windows\system32)



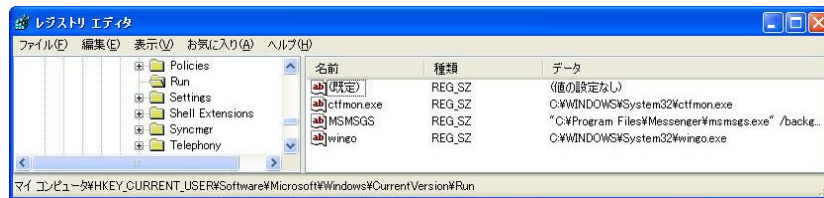
2. レジストリキーを追加する。

Windows の起動時にワームが実行するために次の値を

"wingo" = "%System%\%wingo.exe"

次のレジストリキーに追加する。

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run



次の値を

"Timekey" = "[乱数]"

次のレジストリキーに追加する。

HKEY_CURRENT_USER\Software\Microsoft\Params



3. 次のプロセスを終了する。

mcagent.exe
 mcvsshld.exe
 mcshield.exe
 mcvsescn.exe
 mcvsrte.exe
 DefWatch.exe
 Rtvsan.exe
 ccEvtMgr.exe
 NISUM.EXE
 ccPxySvc.exe
 navapvc.exe
 NPROTECT.EXE
 nopdb.exe
 ccApp.exe
 Avsynmgr.exe
 VsStat.exe
 Vshwin32.exe

alogserv.exe
RuLaunch.exe
Avconsol.exe
PavFires.exe
FIREWALL.EXE
ATUPDATER.EXE
LUALL.EXE
DRWEBUPW.EXE
AUTODOWN.EXE
NUPGRADE.EXE
OUTPOST.EXE
ICSSUPPNT.EXE
ICSUPP95.EXE
ESCANH95.EXE
AVXQUAR.EXE
ESCANHNT.EXE
ATUPDATER.EXE
AUPDATE.EXE
AUTOTRACE.EXE
AUTOUPDATE.EXE
AVXQUAR.EXE
AVWUPD32.EXE
AVPUPD.EXE
CFIAUDIT.EXE
UPDATE.EXE
NUPGRADE.EXE
MCUPDATE.EXE
pavsrv50.exe
AVENGINE.EXE
APVXDWIN.EXE
pavProxy.exe
navapw32.exe
navapsvc.exe
ccProxy.exe
navapsvc.exe
NPROTECT.EXE
SAVScan.exe
SNDSrv.exe
symlcsvc.exe
LUCOMS 1.EXE
blackd.exe
bawindo.exe
FrameworkService.exe
VsTskMgr.exe
SHSTAT.EXE
UpdaterUI.exe

4. 次の URL のいずれかからファイルをダウンロードし、%System%#re_file.exe に保存し、実行を試みる。

www.bottombouncer.com
www.bottombouncer.com
www.anthonyflanagan.com
www.bradster.com
www.traverse.com
www.ims-i.com

www.realgps.com
www.aviation-center.de
www.gci-blh.de
www.pankration.com
www.jansenboiler.com
www.corpsite.com
www.everett.wednet.edu
www.onepositiveplace.org
www.raecoinc.com
www.wwwebad.com
www.corpsite.com
www.wwwebmaster.com
www.wwwebad.com
www.dragcar.com
www.wwwebad.com
www.oohlala-kirkland.com
www.calderwoodinn.com
www.buddyboymusic.com
www.smacgreetings.com
www.tkd2xcell.com
www.curtmarsh.com
www.dontbeaweekendparent.com
www.soloconsulting.com
www.lasermach.com
www.generationnow.net
www.flashcorp.com
www.kencorbett.com
www.FritoPie.NET
www.leonhendrix.com
www.transportation.gov.bh
www.transportation.gov.bh
www.jhaforpresident.7p.com
www.DarrkSydebaby.com
www.cntv.info
www.sugardas.lt
www.adhdtests.com
www.argontech.net
www.customloyal.com
www.ohiolimo.com
www.topko.sk
www.alupass.lu
www.sigi.lu
www.redlightpictures.com
www.irinaswelt.de
www.bueroservice-it.de
www.kranenberg.de
www.kranenberg.de
www.the-fabulous-lions.de
www.the-fabulous-lions.de
www.mongolische-renner.de
www.mongolische-renner.de
www.capri-frames.de
www.capri-frames.de
www.aimcenter.net
www.boneheadmusic.com

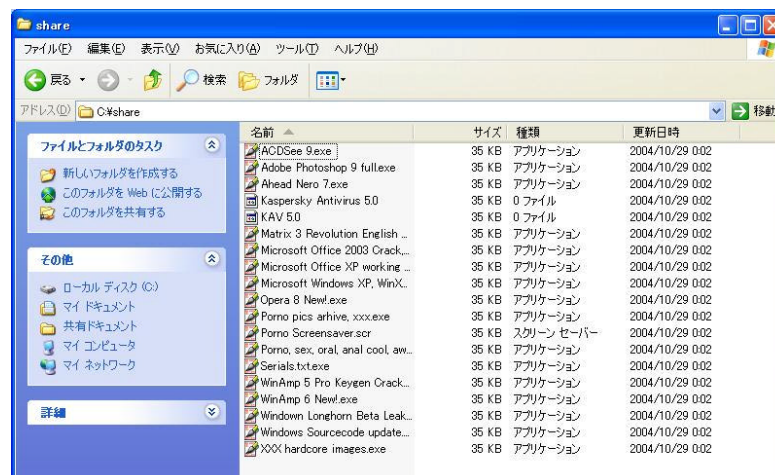
www.fludir.is
www.sljinc.com
www.tivogoddess.com
www.fcpages.com
www.andara.com
www.freeservers.com
www.programmierung2000.de
www.asianfestival.nl
www.aviation-center.de
www.gci-blh.de
www.mass-i.kiev.ua
www.jasnet.pl
www.atlantisteste.hpg.com.br
www.fludir.is
www.rieraquadros.com.br
www.metal.pl
www.handsforhealth.com
www.angelartsanctuary.com
www.firstnightoceancounty.org
www.chinasenfa.com
www.chinasenfa.com
www.ulpiano.org
www.gamp.pl
www.vikingpc.pl
www.woundedshepherds.com
www.cpc.adv.br
www.velocityprint.com
www.esperanzaparalafamilia.com
www.celula.com.mx
www.mexis.com
www.wecompete.com
www.vbw.info
www.gfn.org
www.aegee.org
www.deadrobot.com
www.cscliberec.cz
www.ecofotos.com.br
www.amanit.ru
www.bga-gsm.ru
www.innnewport.com
www.knicks.nl
www.srg-neuburg.de
www.mepmh.de
www.mepbisu.de
www.kradtraining.de
www.polizeimotorrad.de
www.sea.bz.it
www.uslungiarue.it
www.gcnet.ru
www.aimcenter.net
www.vandermost.de
www.vandermost.de
www.szantomierz.art.pl
www.immonaut.sk
www.eurostavba.sk

www.spadochron.pl
www.pyrlandia-boogie.pl
www.kps4parents.com
www.pipni.cz
www.selu.edu
www.travelchronic.de
www.fleigutaetscher.ch
www.irakli.org
www.oboe-online.com
www.oboe-online.com
www.pe-sh.com
www.idb-group.net
www.ceskyhosting.cz
www.ceskyhosting.cz
www.hartacorporation.com
www.glass.la
www.glass.la
www.24-7-transportation.com
www.fepese.ufsc.br
www.ellarouge.com.au
www.bbsh.org
www.boneheadmusic.com
www.sljinc.com
www.tivogoddess.com
www.fcpages.com
www.szantomierz.art.pl
www.elealazar.com
www.ssmifc.ca
www.reliance-yachts.com
www.worest.com.ar
www.kps4parents.com
www.coolfreepages.com
www.scanex-medical.fi
www.jimvann.com
www.orari.net
www.himpsi.org
www.mtfdesign.com
www.jldr.ca
www.relocationflorida.com
www.rentalstation.com
www.approved1stmortgage.com
www.velezcourtesymanagement.com
www.sunassetholdings.com
www.compsolutionstore.com
www.uhcc.com
www.justrepublicans.com
www.pfadfinder-leobersdorf.com
www.featech.com
www.vinirforge.com
www.magicbottle.com.tw
www.giantrevenue.com
www.couponcapital.net
www.crystalrose.ca
www.crystalrose.ca
www.crystalrose.ca

www.crystalrose.ca

5. ハードディスク内の "share" という文字列を含むフォルダを探し出し自分自身をコピーする。作成するファイル名は次のいずれかを使う

Microsoft Office 2003 Crack, Working!.exe
 Microsoft Windows XP, WinXP Crack, working Keygen.exe
 Microsoft Office XP working Crack, Keygen.exe
 Porno, sex, oral, anal cool, awesome!!.exe
 Porno Screensaver.scr
 Serials.txt.exe
 KAV 5.0
 Kaspersky Antivirus 5.0
 Porno pics arhive, xxx.exe
 Windows Sourcecode update.doc.exe
 Ahead Nero 7.exe
 Windown Longhorn Beta Leak.exe
 Opera 8 New!.exe
 XXX hardcore images.exe
 WinAmp 6 New!.exe
 WinAmp 5 Pro Keygen Crack Update.exe
 Adobe Photoshop 9 full.exe
 Matrix 3 Revolution English Subtitles.exe
 ACDSee 9.exe



6. 次のサービスを停止する。
 "SharedAccess" - Internet Connection Sharing
 "wscsvc" - MS security center
7. TCP ポート81 を開き、感染したコンピュータにバックドアを作成する。
8. レジストリの値を削除する。
 次の文字列を含む全ての値を
 My AV
 Zone Labs Client Ex
 9XHtProtect
 Antivirus
 Special Firewall Service
 service
 Tiny AV
 ICQNet

HtProtect
NetDy
Jammer2nd
FirewallSvr
MsInfo
SysMonXP
EasyAV
PandaAVEngine
Norton Antivirus AV
KasperskyAVEng
SkynetsRevenge
ICQ Net

次のレジストリキーから削除する。

HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run

HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run

9. 次の拡張子を持つファイルからメールアドレスを収集する。

.wab
.txt
.msg
.htm
.shtm
.stm
.xml
.dbx
.mbx
.mdx
.eml
.nch
.mmf
.ods
.cfg
.asp
.php
.pl
.wsh
.adb
.tbb
.sht
.xls
.oft
.uin
.cgi
.mht
.dhtm
.jsp

10. 9 で収集したメールアドレスに対し、独自の SMTP エンジンを使用して電子メールを送信する。ただし、次の文字列を含むメールアドレスには送信しない。

@hotmail
@msn
@microsoft
rating@
f-secur
news

	<p>update anyone@ bugs@ contract@ feste gold-certs@ help@ info@ nobody@ noone@ kasp admin icrosoft support ntivi unix bsd linux listserv certific sopho @foo @iana free-av @messagelab winzip google winrar samples abuse panda cafee spam pgp @avp. noreply local root@ postmaster@</p>
感染・発症防止方法	<ol style="list-style-type: none"> 「ウイルスの動作概要」に記述した内容のメールが届いた場合には、容易にメールを開封しない。 予期せぬメールが届いた場合には、添付ファイルを絶対に開かない。
ウイルスの駆除方法	<p>手動による修復を行う場合、コンピュータに関する高度な知識が必要とされ、間違えるとコンピュータが正常に起動しなくなる場合もある。</p> <ol style="list-style-type: none"> 被害拡大防止のため、感染したコンピュータをネットワークから切り離す。 システムの復元オプションを無効にする。(Windows Me/XP) コンピュータをセーフモード(WindowsNT では VGA モード)で再起動する。 感染ファイルを削除する。 次のファイルを削除する。

	<p>%System%\wingo.exe %System%\wingo.exeopen %System%\wingo.exeopenopen %System%\wingo.exeopenopenopen %System%\wingo.exeopenopenopenopen %System%\re_file.exe</p> <p>"shar" という文字列を含むフォルダ内の次のファイルを削除する。 Microsoft Office 2003 Crack, Working!.exe Microsoft Windows XP, WinXP Crack, working Keygen.exe Microsoft Office XP working Crack, Keygen.exe Porno, sex, oral, anal cool, awesome!!.exe Porno Screensaver.scr Serials.txt.exe KAV 5.0 Kaspersky Antivirus 5.0 Porno pics arhive, xxx.exe Windows Sourcecode update.doc.exe Ahead Nero 7.exe Windown Longhorn Beta Leak.exe Opera 8 New!.exe XXX hardcore images.exe WinAmp 6 New!.exe WinAmp 5 Pro Keygen Crack Update.exe Adobe Photoshop 9 full.exe Matrix 3 Revolution English Subtitles.exe ACDSsee 9.exe</p> <p>5. レジストリに行われた変更を元に戻す。 次の値を "wingo" = "%System%\wingo.exe" 次のレジストリキーから削除する。 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</p> <p>次の値を "Timekey" = "[乱数]" 次のレジストリキーから削除する。 HKEY_CURRENT_USER\Software\Microsoft\Params</p> <p>各操作については Microsoft のホームページ、付属のマニュアル等を参照すること。</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	無