

ウイルス解析報告書

ウイルス名	W32.Beagle.X@mm ([-Worm.Bagle.z [Kaspersky], WORM_BAGLE.Z [Trend], WORM_BAGLE.AA [Trend], WORM_BAGLE.AB [Trend], W32/Bagle.aa@MM [McAfee], W32/Bagle.ab@MM [McAfee], W32/Bagle-AA [Sophos], Win32.Bagle.X [Computer Associates])
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	不明
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 4 月 28 日
発見場所	ドイツ (最初の感染報告)
危険性	感染力が強い。短時間で多くの届出が寄せられた。危険度は5段階の3(5が最も危険)。
発症条件	ワームによって送信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 エンジンを使用した電子メール及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バックドアを開く、自身の最後尾にランダムなデータを付加するため、固定の MD5 値を持たない。
被害の規模	発見から 55 時間で 1678 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 (2004 年 1月 18 日発見)以降多数の亜種、変種が発見されている。
ウイルスの動作概要	<p>ワームによって送信されるメールには次のような特徴がある。</p> <p>差出人 詐称されている。</p> <p>件名 次のうち、いずれかを使用する。</p> <ul style="list-style-type: none"> Re: Msg reply Re: Hello Re: Yahoo! Re: Thank you! Re: Thanks :) RE: Text message Re: Document Incoming message Re: Incoming Message RE: Incoming Msg RE: Message Notify Notification Changes.. New changes Hidden message Fax Message Received Protected message RE: Protected message Forum notify Site changes Re: Hi Encrypted document

本文 添付ファイルが.zip の場合、本文は、次のいずれかのメッセージを含む。

For security reasons attached file is password protected. The password is

For security purposes the attached file is password protected. Password --

Note: Use password

Attached file is protected with the password for security reasons. Password is

In order to read the attach you have to use the following password:

Archive password:

Password

Password:

ただし、添付ファイルが .zip でない場合、本文は空白となる。

添付ファイル名：

次のうち、いずれかを使用する。

Information

Details

text_document

Readme

Document

Info

the_message

Details

MoreInfo

Message

You_will_answer_to_me

Half_Live

Counter_strike

Loves_money

the_message

Alive_condom

Joke

Toy

Nervous_illnesses

Manufacture

You_are_dismissed

Your_complaint

Your_money

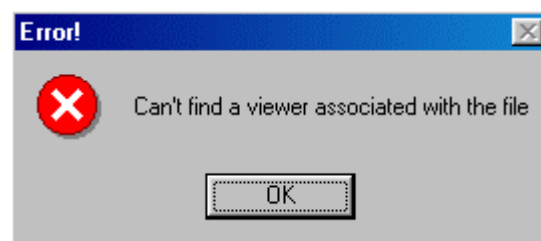
Smoke

I_search_for_you



W32.Beagle.X@mm **が実行されると、次のことを行う**

1. 次のメッセージを表示する。



2. 次の名前のミュートックスを 7 個作成する。これは、W32.Netsky@mm (および幾つかの亜種)の実行を妨害する。

- MuXxXxTENYKSDesignedAsTheFollowerOfSkynet-D
- 'D'r'o'p'p'e'd'S'k'y'N'e't'
- _-oOaxXi!-+S+-+k+-+y+-+N+-+e+-+t+-!XxKoo- _
- [SkyNet.cz]SystemsMutex
- AdmSkynetJkIS003
- __--->>>U<<<<--__
- _-oO]xXi-S-k-y-N-e-t-iXx[Oo- _

3. レジストリの値を削除する。

次の文字列を含む値を

- "My AV"
- "Zone Labs Client Ex"
- "9XHtProtect"
- "Antivirus"
- "Special Firewall Service"

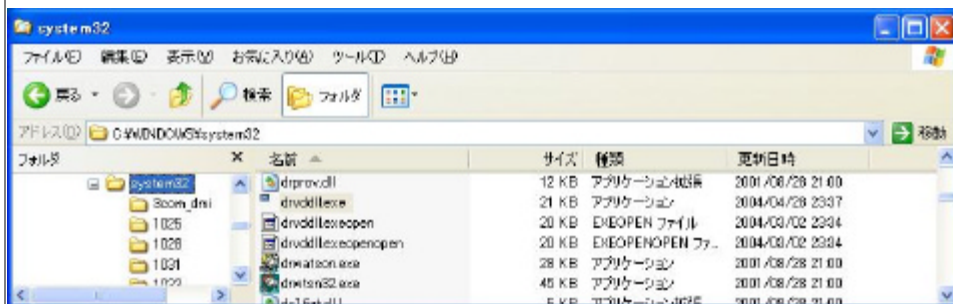
"service"
 "Tiny AV"
 "ICQNet"
 "HtProtect"
 "NetDy"
 "Jammer2nd"
 "FirewallSvr"
 "MslInfo"
 "SysMonXP"
 "EasyAV"
 "PandaAVEngine"
 "Norton Antivirus AV"
 "KasperskyAVEng"
 "SkynetsRevenge"
 "ICQ Net"

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
 これらの値は、W32.Netsky@mm (および幾つかの亜種)により追加される。

4. ワーム自身を %System%\%drvddll.exe としてコピーする。

%System%は不定で、標準設定では C:\Windows\System (Windows 95/98/Me)、
 C:\Winnt\System32 (Windows NT/2000)、あるいは C:\Windows\System32 (Windows
 XP)となる。



5. ワーム自身のコピーにランダムなデータを付加し、%System%\%drvddll.exeopen として作成する。

6. %System%\%drvddll.exeopenopen を作成する。このファイルは、.zip ファイル、.vbs ファイル、.cpl ファイル、.hta ファイル、またはワーム自身の場合がある。ファイルタイプにより、次の動作を行う。

・zip ファイルの場合

ランダムな名前のファイルを2つ含んでいる。1つは .exe ファイルであり、もう1つは .sys、.dat、.idx、.vxd、.vid、あるいは .dll を拡張子を持つテキストファイルである。

・vbs ファイルの場合

%System% フォルダに vss_2.exe という名前のファイルを作成する。

・cpl ファイルの場合

%Windir%フォルダに cplstub.exe という名前のファイルを作成する。

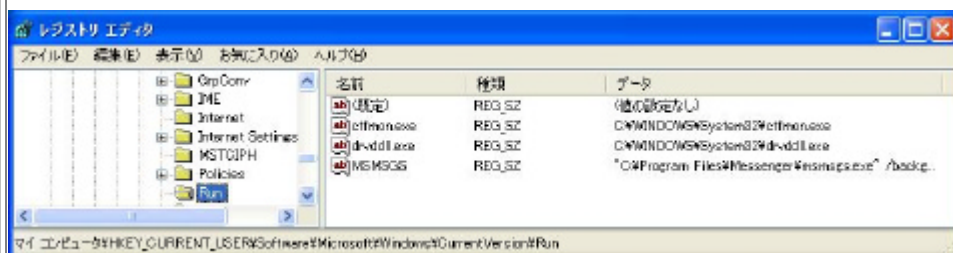
・hta ファイルの場合

%System% フォルダに qwrk.exe という名前のファイルを作成する。

7. %System%\%drvddll.exeopenopenopen を作成する。感染したコンピュータ上に adiplus.dll がある場合、このファイルの拡張子は .ipa あるいは .aif、無い場合は .bmp

である。

8. %System%¥drvdll.exeopenopenopenopen を作成する。このファイルは、6 文字のランダムな文字を含むテキストファイルである。
9. Windows 起動時にワームが実行されるようにレジストリキーを追加する。
次の値を
"Drvdll_exe"="%system%¥drvdll.exe"
次のレジストリキーに追加する。
HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run



10. TCP ポート2535 を開き、感染したコンピュータにバックドアを作成する。
11. 感染したコンピュータの固定ドライブをスキャンし、感染したコンピュータ上の "shar" という文字を含む全フォルダに対し、自身の複製を作成しようとする。複製するファイル名は、次のようになる。
 - 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
 - Window 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



12. 次の拡張子を持つファイルから電子メールアドレスを収集し、発見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付する。

.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

添付ファイルの拡張子は、drvddll.exeopenopen と同じタイプになる。例えば、drvddll.exeopenopen が.zip ファイルとして作成された場合、添付ファイルは、.zip ファイルになる。drvddll.exeopenopen がワーム自身であった場合、拡張子は、.exe、.com、あるいは .scr になる。

13. 次のいずれかのドメインにおける .php スクリプトへのアクセスを試みる。

<http://www.spiegel.de/>
<http://www.leipziger-messe.de/>
<http://www.mobile.de/>
<http://www.neformal.de/>
<http://www.avh.de/>
<http://www.goethe.de/>
<http://www.degruyter.de/>
<http://www.heise.de/>
<http://www.autoscout24.de/>
<http://www.russische-botschaft.de/>
<http://www.bmbf.de/>
<http://www.berlinale.de/>
<http://www.hamann-motorsport.de/>
<http://Spaceclub.de/>
<http://www.fracht-24.de/>
<http://www.loveparade.de/>

<http://www.dalnoboysnik.de/>
<http://www.deutschland.de/>
<http://www.ac-schnitzer.de/>
<http://abakan.strana.de/>
<http://www.emis.de/>
<http://www.dwd.de/>
<http://www.ifdesign.de/>
<http://www.beckers-systems.de/>
<http://www.pri-wo-hamburg.de/>
<http://virtualzone.de/>
<http://www.mitsumi.de/>
<http://www.fu-berlin.de/>
<http://www.nabu.de/>
<http://www.tekeli.de/>
<http://www.welt.de/>
<http://www.gospel-nations.de/>
<http://www.neznakomez.de/>
<http://www.tecchannel.de/>
<http://www.php-resource.de/>
<http://www.windac.de/>
<http://www.gsi.de/>
<http://www.turism.de/>
<http://jakimov.golos.de/>
<http://www.www.mirko-becker.gmxhome.de/>
<http://vg.xtonne.de/>
<http://www.go-amman.de/>
<http://3treepoint.com/>
<http://www.restarted-alliance.de/>
<http://2udar.ligakvn.de/>
<http://www.sprach-zertifikat.de/>
<http://www.dfg.de/>
<http://www.kliniken.de/>
<http://www.winfuture.de/>
<http://www.hamburg.de/>
<http://www.auma.de/>
<http://www.teac.de/>
<http://www.eumetsat.de/>
<http://www.documenta.de/>
<http://hardvision.ru/>
<http://www.bruecke-osteuropa.de/>
<http://www.mk-motorsport.de/>
<http://www.bundesregierung.de/>
<http://ditec.um.es/>
<http://www.insel-ruegen-hotel.de/>
<http://www.tib.uni-hannover.de/>
<http://www.chugai.de/>
<http://www.blauer-engel.de/>
<http://www.partner-inform.de/>
<http://mhv24.de/>
<http://villakinderbunt.de/>
<http://s318.evanzo-server.de/>
<http://andimeisslein.de/>
<http://tobimayer.de/>
<http://markusgimenez.de/>
<http://www.fiz-karlsruhe.de/>

<http://www.gdch.de/>
<http://www.intermatgmbh.de/>
<http://www.hotel-pension-spree.de/>
<http://vg.xtonne.de/>
<http://www.low-spirit.de/>
<http://www.red-dot.de/>
<http://www.fernuni-hagen.de/>
<http://www.ruletka.de/>
<http://www.deutsch-als-fremdsprache.de/>
<http://www.uni-oldenburg.de/>
<http://fotos.schneider.bards.de/>
<http://www.deutsches-museum.de/>
<http://www.de-bug.de/>
<http://www.uni-stuttgart.de/>
<http://www.embl-heidelberg.de/>
<http://www.mdz-moskau.de/>
<http://www.mitsubishi-evs.de/>
<http://www.siegenia-aubi.com/>
<http://www.cicv.fr/>
<http://www.paromi.de/>
<http://www.jura.uni-sb.de/>
<http://www.exactaudiocopy.de/>

14. 次のプロセスの強制終了を試みる。

AGENTSVR.EXE
ANTI-TROJAN.EXE
ANTI-TROJAN.EXE
ANTIVIRUS.EXE
ANTS.EXE
APIMONITOR.EXE
APLICA32.EXE
APVXDWIN.EXE
ATCON.EXE
ATGUARD.EXE
ATRO55EN.EXE
ATUPDATER.EXE
ATWATCH.EXE
AUPDATE.EXE
AUTODOWN.EXE
AUTOTRACE.EXE
AUTOUPDATE.EXE
AVCONSOL.EXE
AVGSERV9.EXE
AVLTMAIN.EXE
AVprotect9x.exe
AVPUPD.EXE
AVSYNMGR.EXE
AVWUPD32.EXE
AVXQUAR.EXE
BD_PROFESSIONAL.EXE
BIDF.EXE
BIDSERVER.EXE
BIPCP.EXE
BIPCPEVALSETUP.EXE
BISP.EXE

BLACKD.EXE
BLACKICE.EXE
BOOTWARN.EXE
BORG2.EXE
BS120.EXE
CDP.EXE
CFGWIZ.EXE
CFGWIZ.EXE
CFIADMIN.EXE
CFIADMIN.EXE
CFIAUDIT.EXE
CFIAUDIT.EXE
CFIAUDIT.EXE
CFINET.EXE
CFINET.EXE
CFINET32.EXE
CFINET32.EXE
CLEAN.EXE
CLEAN.EXE
CLEANER.EXE
CLEANER.EXE
CLEANER3.EXE
CLEANPC.EXE
CLEANPC.EXE
CMGRDIAN.EXE
CMGRDIAN.EXE
CMON016.EXE
CMON016.EXE
CPD.EXE
CPF9X206.EXE
CPFNT206.EXE
CV.EXE
CWNB181.EXE
CWNTDWMO.EXE
DEFWATCH.EXE
DEPUTY.EXE
DPF.EXE
DPFSETUP.EXE
drvsys.exe
DRWATSON.EXE
DRWEBUPW.EXE
ENT.EXE
ESCANH95.EXE
ESCANHNT.EXE
ESCANV95.EXE
EXANTIVIRUS-CNET.EXE
FAST.EXE
FIREWALL.EXE
FLOWPROTECTOR.EXE
FP-WIN_TRIAL.EXE
FRW.EXE
FSAV.EXE
FSAV530STBYB.EXE
FSAV530WTBYB.EXE
FSAV95.EXE

GBMENU.EXE
GBPOLL.EXE
GUARD.EXE
GUARDDOG.EXE
HACKTRACERSETUP.EXE
HTLOG.EXE
HWPE.EXE
IAMAPP.EXE
IAMAPP.EXE
IAMSERV.EXE
ICLOAD95.EXE
ICLOADNT.EXE
ICMON.EXE
ICSSUPPNT.EXE
ICSUPP95.EXE
ICSUPP95.EXE
ICSUPPNT.EXE
IFW2000.EXE
IPARMOR.EXE
IRIS.EXE
JAMMER.EXE
KAVLITE40ENG.EXE
KAVPERS40ENG.EXE
KERIO-PF-213-EN-WIN.EXE
KERIO-WRL-421-EN-WIN.EXE
KERIO-WRP-421-EN-WIN.EXE
KILLPROCESSSETUP161.EXE
LDPRO.EXE
LOCALNET.EXE
LOCKDOWN.EXE
LOCKDOWN2000.EXE
LSETUP.EXE
LUALL.EXE
LUCOMSERVER.EXE
LUNIT.EXE
MCAGENT.EXE
MCUPDATE.EXE
MCUPDATE.EXE
MFW2EN.EXE
MFWENG3.02D30.EXE
MGUI.EXE
MINILOG.EXE
MOOLIVE.EXE
MRFLUX.EXE
MSCONFIG.EXE
MSINFO32.EXE
MSSMMC32.EXE
MU0311AD.EXE
NAV80TRY.EXE
NAVAPW32.EXE
NAVDX.EXE
NAVSTUB.EXE
NAVW32.EXE
NC2000.EXE
NCINST4.EXE

NDD32.EXE
NEOMONITOR.EXE
NETARMOR.EXE
NETINFO.EXE
NETMON.EXE
NETSCANPRO.EXE
NETSPYHUNTER-1.2.EXE
NETSTAT.EXE
NISSERV.EXE
NISUM.EXE
NMAIN.EXE
NORTON_INTERNET_SECU_3.0_407.EXE
NPF40_TW_98_NT_ME_2K.EXE
NPFMESSENGER.EXE
NPROTECT.EXE
NSCHED32.EXE
NTVDM.EXE
NUPGRADE.EXE
NVARCH16.EXE
NWINST4.EXE
NWTOOL16.EXE
OSTRONET.EXE
OUTPOST.EXE
OUTPOSTINSTALL.EXE
OUTPOSTPROINSTALL.EXE
PADMIN.EXE
PANIXK.EXE
PAVPROXY.EXE
PCC2002S902.EXE
PCC2K_76_1436.EXE
PCCIOMON.EXE
PCDSETUP.EXE
PCFWALLICON.EXE
PCFWALLICON.EXE
PCIP10117.0.EXE
PDSETUP.EXE
PERISCOPE.EXE
PERSFW.EXE
PF2.EXE
PFWADMIN.EXE
PINGSCAN.EXE
PLATIN.EXE
POPROXY.EXE
POPSCAN.EXE
PORTDETECTIVE.EXE
PPINUPDT.EXE
PPTBC.EXE
PPVSTOP.EXE
PROCEXPLORERV1.0.EXE
PROPORT.EXE
PROTECTX.EXE
PSPF.EXE
PURGE.EXE
PVIEW95.EXE
QCONSOLE.EXE

QSERVER.EXE
RAV8WIN32ENG.EXE
REGEDIT.EXE
REGEDT32.EXE
RESCUE.EXE
RESCUE32.EXE
RRGUARD.EXE
RSHELL.EXE
RTVSCN95.EXE
RULAUNCH.EXE
SAFEWEB.EXE
SBSERV.EXE
SD.EXE
SETUP_FLOWPROTECTOR_US.EXE
SETUPVAMEEVAL.EXE
SFC.EXE
SGSSFW32.EXE
SH.EXE
SHELLSPYINSTALL.EXE
SHN.EXE
SMC.EXE
SOFI.EXE
SPF.EXE
SPHINX.EXE
SPYXX.EXE
SS3EDIT.EXE
ST2.EXE
SUPFTRL.EXE
SUPPORTER5.EXE
SYMPROXYSVC.EXE
SYSEDIT.EXE
TASKMON.EXE
TAUMON.EXE
TAUSCAN.EXE
TC.EXE
TCA.EXE
TCM.EXE
TDS2-98.EXE
TDS2-NT.EXE
TDS-3.EXE
TFAK5.EXE
TGBOB.EXE
TITANIN.EXE
TITANINXP.EXE
TRACERT.EXE
TRJSCAN.EXE
TRJSETUP.EXE
TROJANTRAP3.EXE
UNDOBOOT.EXE
UPDATE.EXE
VBCMSERV.EXE
VBCONS.EXE
VBUST.EXE
VBWIN9X.EXE
VBWINNTW.EXE

	<p>VCSETUP.EXE VFSETUP.EXE VIRUSMDPERSONALFIREWALL.EXE VNLAN300.EXE VNPC3000.EXE VPC42.EXE VPFW30S.EXE VPTRAY.EXE VSCENU6.02D30.EXE VSECOMR.EXE VSHWIN32.EXE VSISSETUP.EXE VSMAN.EXE VSMON.EXE VSSTAT.EXE VSWIN9XE.EXE VSWINNTSE.EXE VSWINPERSE.EXE W32DSM89.EXE W9X.EXE WATCHDOG.EXE WEBSCANX.EXE WGFE95.EXE WHOSWATCHINGME.EXE WHOSWATCHINGME.EXE WINRECON.EXE WNT.EXE WRADMIN.EXE WRCTRL.EXE WSBGATE.EXE WYVERNWORKSFIREWALL.EXE XPF202EN.EXE ZAPRO.EXE ZAPSETUP3001.EXE ZATUTOR.EXE ZAUINST.EXE ZONALM2601.EXE ZONEALARM.EXE</p> <p>15. システムの日付が 2005 年 1 月 25 日以降の場合、ワームは直ちに感染活動を中止し、自分自身のレジストリ値、および次のレジストリキーを削除する。 HKEY_CURRENT_USER¥SOFTWARE¥Time 次のレジストリキーの HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run 次の値を削除する。 "Drvddll_exe" = "%system%¥drvddll.exe"</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ります。</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。

	<ol style="list-style-type: none">2. システムの復元オプションを無効にする (Windows Me/XP)3. 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4. 感染ファイルを削除する %System%¥drvddll.exe5. レジストリに行われた変更を元に戻す 次の値を "Drvddll_exe" = "%system%¥drvddll.exe" 次のレジストリキーから削除する。 HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run <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