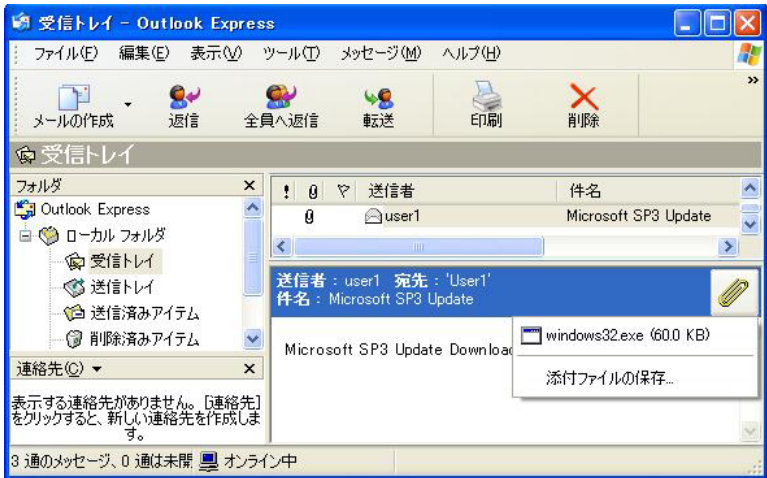


## ウイルス解析報告書

<b>ウイルス名</b>	W32.Rants.B@mm (別名 : Email-Worm.Win32.generic [Kaspersky Lab], W32/Generic.m [McAfee], W32/FlyVB-C [Sophos], WORM_FATSO.F [Trend Micro])
<b>プログラム名及び容量 (添付ファイル名)</b>	プログラム名 : windows32.exe 容 量 : 59,946 バイト
<b>種別</b>	ワーム
<b>プログラム言語</b>	Visual Basic
<b>発症環境</b>	Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP
<b>発見日</b>	2005 年 7 月 18 日
<b>発見場所</b>	アメリカ合衆国
<b>危険性</b>	感染力が高い。危険度は 5 段階の 2 (5 が最も危険)。
<b>発症条件</b>	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。また、W32.Reatle@mm によりプログラムを実行したとき。
<b>ウイルスの活動、影響</b>	このワームは、Microsoft Outlook、MSN Messenger、America Online を使用して拡散する大量メールワームである。また、セキュリティ関連プロセスを停止したり、Windows のセキュリティ機能を無効にしたりする。
<b>被害の規模</b>	発見から 2 日間で 6 件の届出がシマンテック社に寄せられている。
<b>亜種、変種の有無</b>	W32.Rants.A@mm (2005 年 7 月 10 日発見)
<b>ウイルスの動作概要</b>	<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>The screenshot shows the Outlook Express interface. The main pane displays an email from 'user1' with the subject 'Microsoft SP3 Update'. A context menu is open over the attachment 'windows32.exe (60.0 KB)', with the option '添付ファイルの保存...' (Save attachment...) selected. The folder pane on the left shows the '受信トレイ' (Inbox) folder selected.</p>
<b>差出人:</b>	<p>次のいずれかを使用する。</p> <ul style="list-style-type: none"> <li>• update@symantec.com</li> <li>• update@microsoft.com</li> <li>• [ローカルユーザのアドレス]</li> </ul>
<b>件名:</b>	<p>次のいずれかを使用する。</p> <ul style="list-style-type: none"> <li>• Microsoft SP3 Update</li> <li>• Latest update [service pack 3]</li> <li>• Fwd: Microsoft SP3 Update</li> <li>• Latest Update</li> </ul>
<b>本文:</b>	

次のいずれかを使用する。

- Microsoft SP3 Update Download It
- Update your computer with the latest services pack from microsoft

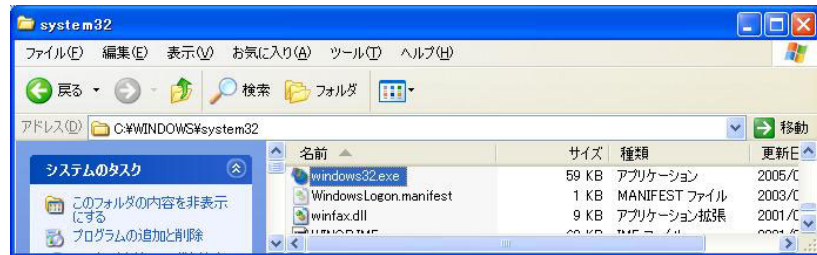
#### 添付ファイル:

次のいずれかを使用する。

- windows32.EXE
- SP3 UPDATE.EXE

このワームが実行されると、次のことを行う。

1. ワーム自身を%System%¥windows32.exeとしてコピーする。



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. Windows の起動時にワームを実行させるため、次のレジストリキーに HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run 次の値を追加する。

"services" = "%System%¥windows32.exe"



Windows のセキュリティ機能を無効にするために、次のレジストリキーの

HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥security center  
HKEY\_CURRENT\_USER¥Software¥Microsoft¥security center

次の値を変更する。

"FirewallDisableNotify" = "1"  
"UpdatesDisableNotify" = "1"  
"AntiVirusDisableNotify" = "1"  
"FirewallDisableNotify" = "1"  
"UpdatesDisableNotify" = "1"  
"AntiVirusDisableNotify" = "1"

Windows のセキュリティ機能を無効にするために、次のレジストリキーの

KEY\_CURRENT\_USER¥Software¥Policies¥Microsoft¥Windows¥  
WindowsUpdate¥AU

次の値を変更する。

"NoAutoUpdate" = "1"

Windows のセキュリティ機能を無効にするために、次のレジストリキーの  
 HKEY\_CURRENT\_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥  
 Policies¥Explorer¥DisallowRun  
 HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥  
 Policies¥Explorer¥DisallowRun

次の値を変更する。

"NMain.exe" = "1"  
 "taskmgr.exe" = "1"  
 "ZLCLIENT.EXE" = "1"

Windows のセキュリティ機能を無効にするために、次のレジストリキーの  
 HKEY\_CURRENT\_USER¥Software¥Microsoft¥Windows NT¥  
 CurrentVersion¥systemrestore  
 HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows NT¥  
 CurrentVersion¥systemrestore

次の値を変更する。

"DisableSR" = "1"

Windows タスクマネージャおよびレジストリ編集ツールを無効にするために、次の  
 レジストリキーの

HKEY\_CURRENT\_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥  
 Policies¥System

次の値を変更する。

"DisableTaskMgr" = "1"  
 "DisableRegistryTools" = "1"

コンピュータ名を"Snart"に変更するために、次のレジストリキーの  
 HKEY\_CURRENT\_USER¥SYSTEM¥CurrentControlSet¥Control¥  
 ComputerName¥ActiveComputerName  
 HKEY\_LOCAL\_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥  
 ComputerName¥ActiveComputerName

次の値を変更する。

"computername" = "Snart"

### 3. 特定のプロセスを停止する。(一部のプロセスはセキュリティに関係している。)

注意: \*は任意の 1 文字を示す。

- \_AVPM.EXE
- \_AVPCC.EXE
- ACKWIN32.EXE
- AckWin32.EXE
- ADVXDWIN.EXE
- AGENTSVR.EXE
- agentw.EXE
- ALERTSVC.EXE
- ALOGSERV.EXE
- AMON9X.EXE
- ANTI-TROJAN.EXE
- ANTIVIRUS.EXE
- ANTS.EXE
- APIMONITOR.EXE
- APLICA32.EXE
- apvxdwin.EXE
- APVXDWIN.EXE
- ATCON.EXE
- ATGUARD.EXE

- ATRO55EN.EXE
- ATUPDATER.EXE
- ATWATCH.EXE
- AUPDATE.EXE
- AUTODOWN.EXE
- AutoTrace.EXE
- AUTOUPDATE.EXE
- AVCONSOL.EXE
- AVGCC32.EXE
- Avgctrl.EXE
- AVGCTRL.EXE
- AvgServ.EXE
- AVGSERV.EXE
- AVGSERV9.EXE
- AVGW.EXE
- avkpop.EXE
- AvkServ.EXE
- avkservice.EXE
- avkwctl9.EXE
- AVP.EXE
- AVP32.EXE
- AVPCC.EXE
- AVPM.EXE
- avpm.EXE
- Avsched32.EXE
- AVSYNMGR.EXE
- AVWINNT.EXE
- AVXMONITOR9X.EXE
- AVXMONITORNT.EXE
- AVXQUAR.EXE
- AVXQUAR.EXE
- AVXW.EXE
- BD\_PROFESSIONAL.EXE
- BIDEF.EXE
- BIDSERVER.EXE
- BIPCP.EXE
- BIPCPEVALSETUP.EXE
- BISP.EXE
- BLACKD.EXE
- blackd.EXE
- BLACKICE.EXE
- BlackICE.EXE
- BOOTWARN.EXE
- BORG2.EXE
- BS120.EXE
- ccApp.EXE
- ccEvtMgr.EXE
- ccPxySvc.EXE
- CDP.EXE
- CFGWIZ.EXE
- CFIADMIN.EXE
- CFIAUDIT.EXE
- CFINET.EXE
- CFINET32.EXE
- cleaner3.EXE

- CLEANPC.EXE
- CMGRDIAN.EXE
- CMON016.EXE
- CONNECTIONMONITOR.EXE
- CPD.EXE
- cpd.EXE
- Claw95.EXE
- CLAW95CF.EXE
- Claw95cf.EXE
- CLEAN.EXE
- CLEANER.EXE
- cleaner.EXE
- CLEANER3.EXE
- CPF9X206.EXE
- CPFNT206.EXE
- CTRL.EXE
- CV.EXE
- CV.EXE
- CWNB181.EXE
- CWNTDWMO.EXE
- defalert.EXE
- defscangui.EXE
- DEFWATCH.EXE
- DEPUTY.EXE
- DOORS.EXE
- DPF.EXE
- DPFSETUP.EXE
- DRWATSON.EXE
- DRWEB32.EXE
- DVP95.EXE
- DVP95\_0.EXE
- EFPEADM.EXE
- ENT.EXE
- ESCANH95.EXE
- ESCANHNT.EXE
- ESCANV95.EXE
- ETRUSTCIPE.EXE
- ETRUSTCIPE.EXE
- EVPN.EXE
- EXANTIVIRUS-CNET.EXE
- EXPERT.EXE
- F-AGNT95.EXE
- fameh32.EXE
- FAST.EXE
- fch32.EXE
- fih32.EXE
- FIREWALL.EXE
- FLOWPROTECTOR.EXE
- fnrb32.EXE
- F-PROT.EXE
- F-PROT95.EXE
- FP-WIN.EXE
- FP-WIN\_TRIAL.EXE
- FRW.EXE
- fsaa.EXE

- FSAV.EXE
- fsav32.EXE
- FSAV530STBYB.EXE
- FSAV530WTBYB.EXE
- FSAV95.EXE
- fsgk32.EXE
- fsm32.EXE
- fsma32.EXE
- fsmb32.EXE
- F-STOPW.EXE
- f-stopw.EXE
- GBMENU.EXE
- gbmenu.EXE
- gbpoll.EXE
- GBPOLL.EXE
- GENERICS.EXE
- GUARD.EXE
- GUARDDOG.EXE
- HACKTRACERSETUP.EXE
- HTLOG.EXE
- HWPE.EXE
- IAMAPP.EXE
- iamapp.EXE
- IAMSERV.EXE
- iamserv.EXE
- IAMSTATS.EXE
- ICLOAD95.EXE
- ICLOADNT.EXE
- ICMON.EXE
- ICSUPP95.EXE
- ICSUPPNT.EXE
- IFACE.EXE
- IFW2000.EXE
- IOMON98.EXE
- IPARMOR.EXE
- IRIS.EXE
- ISRV95.EXE
- JAMMER.EXE
- JEDI.EXE
- KAVLITE40ENG.EXE
- KAVPERS40ENG.EXE
- KAVPF.EXE
- KERIO-PF-213-EN-WIN.EXE
- KERIO-WRL-421-EN-WIN.EXE
- KERIO-WRP-421-EN-WIN.EXE
- KILLPROCESSSETUP161.EXE
- LDNETMON.EXE
- LDPRO.EXE
- LDPROMENU.EXE
- LDSCAN.EXE
- LOCALNET.EXE
- LOCKDOWN.EXE
- LOCKDOWN2000.EXE
- lockdown2000.EXE
- LSETUP.EXE

- LUALL.EXE
- LUAU.EXE
- LUCOMSERVER.EXE
- LUINIT.EXE
- LUSPT.EXE
- MCAAGENT.EXE
- MCMNHDLR.EXE
- Mcshield.EXE
- MCTOOL.EXE
- MCUPDATE.EXE
- MCVSRTE.EXE
- MCVSSHLD.EXE
- MFW2EN.EXE
- MFWENG3.02D30.EXE
- MGAVRTCL.EXE
- MGAVRTE.EXE
- MGHTML.EXE
- MGUI.EXE
- MINILOG.EXE
- MONITOR.EXE
- Monitor.EXE
- MOOLIVE.EXE
- MPFAGENT.EXE
- MPFSERVICE.EXE
- MPFTRAY.EXE
- MRFLUX.EXE
- MSCONFIG.EXE
- MSINFO32.EXE
- MSSMMC32.EXE
- MU0311AD.EXE
- MWATCH.EXE
- MWATCH.EXE
- NAV80TRY.EXE
- navapsvc.EXE
- NAVAPSVG.EXE
- NAVAPW32.EXE
- NAVDX.EXE
- NAVLU32.EXE
- NAVSTUB.EXE
- NAVW32.EXE
- Navw32.EXE
- NAVWNT.EXE
- NC2000.EXE
- NCINST4.EXE
- NDD32.EXE
- NEOMONITOR.EXE
- NeoWatchLog.EXE
- NETARMOR.EXE
- NETARMOR.EXE
- NETINFO.EXE
- NETMON.EXE
- NETSCANPRO.EXE
- NETSPYHUNTER-1.2.EXE
- NETSTAT.EXE
- NETUTILS.EXE

- NISSERV.EXE
- NISUM.EXE
- NMAIN.EXE
- NORMIST.EXE
- NORTON\_INTERNET\_SECU\_3.0\_407.EXE
- notstart.EXE
- NPF40\_TW\_98\_NT\_ME\_2K.EXE
- NPFMESSENGER.EXE
- NPROTECT.EXE
- npscheck.EXE
- NPSSVC.EXE
- NSCHED32.EXE
- ntrtscan.EXE
- NTVDM.EXE
- NTXconfig.EXE
- Nui.EXE
- Nupgrade.EXE
- NVARCH16.EXE
- NVC95.EXE
- nvsvc32.EXE
- NWINST4.EXE
- NWService.EXE
- NWTOOL16.EXE
- OSTRONET.EXE
- OUTPOST.EXE
- OUTPOSTINSTALL.EXE
- OUTPOSTPROINSTALL.EXE
- PADMIN.EXE
- PANIXK.EXE
- pavproxy.EXE
- PAVPROXY.EXE
- PCC2002S902.EXE
- PCC2K\_76\_1436.EXE
- PCCIOMON.EXE
- pccntmon.EXE
- pccwin97.EXE
- PCCWIN98.EXE
- PCDSETUP.EXE
- PCFWALLICON.EXE
- PCFWALLICON.EXE
- PCIP10117\_0.EXE
- pcscan.EXE
- PDSETUP.EXE
- PERISCOPE.EXE
- PERSFW.EXE
- PERSWF.EXE
- PF2.EXE
- PFWADMIN.EXE
- PINGSCAN.EXE
- PLATIN.EXE
- POP3TRAP.EXE
- POPROXY.EXE
- POPSCAN.EXE
- PORTDETECTIVE.EXE
- PORTMONITOR.EXE

- PPINUPDT.EXE
- PPTBC.EXE
- PPVSTOP.EXE
- PROCESSMONITOR.EXE
- PROCEXPLORERV1.0.EXE
- PROGRAMAUDITOR.EXE
- PROPORT.EXE
- PROTECTX.EXE
- PSPF.EXE
- PURGE.EXE
- PVIEW95.EXE
- QCONSOLE.EXE
- QSERVER.EXE
- rapapp.EXE
- RAV7.EXE
- RAV7WIN.EXE
- RAV8WIN32ENG.EXE
- REALMON.EXE
- REGEDIT.EXE
- REGEDT32.EXE
- RESCUE.EXE
- RESCUE32.EXE
- RRGUARD.EXE
- RSHELL.EXE
- RTVSCN95.EXE
- RULAUNCH.EXE
- SAFEWEB.EXE
- SBSERV.EXE
- sbserv.EXE
- SCAN32.EXE
- SCRSCAN.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
- Sphinx.EXE
- SPYXX.EXE
- SS3EDIT.EXE
- ST2.EXE
- SUPFTRL.EXE
- SUPPORTER5.EXE
- SWEEP95.EXE
- SweepNet
- SWEEPSRV.SYS
- SWNETSUP.EXE
- SYMPROXYSVC.EXE
- SymProxySvc.EXE

- SYMTRAY.EXE
- SYSEDIT.EXE
- TASKMON.EXE
- TAUMON.EXE
- TC.EXE
- TCA.EXE
- TCM.EXE
- TDS2-98.EXE
- TDS2-NT.EXE
- TDS-3.EXE
- TFAK.EXE
- TFAK5.EXE
- TGBOB.EXE
- TITANIN.EXE
- TITANINXP.EXE
- TRACERT.EXE
- TRJSCAN.EXE
- TRJSETUP.EXE
- TROJANTRAP3.EXE
- UNDOBOOT.EXE
- UPDATE.EXE
- VBCMSERV.EXE
- vbcmserv.EXE
- rtvscan.EXE
- VBCONS.EXE
- VbCons.EXE
- VBUST.EXE
- VBWIN9X.EXE
- VBWINNTW.EXE
- VCSETUP.EXE
- VET32.EXE
- VET32.EXE
- VET95.EXE
- Vet95.EXE
- VETTRAY.EXE
- VetTray.EXE
- VFSETUP.EXE
- VIR-HELP.EXE
- VIRUSMDPERSONALFIREWALL.EXE
- VNLAN300.EXE
- VNPC3000.EXE
- VPC32.EXE
- VPC42.EXE
- VPFW30S.EXE
- VPTRAY.EXE
- VSCENU6.02D30.EXE
- VSCHED.EXE
- VSECOMR.EXE
- vshwin32.EXE
- VSISSETUP.EXE
- VSMAIN.EXE
- VSMON.EXE
- vsmon.EXE
- VSSTAT.EXE
- VSWIN9XE.EXE

- VSWINNTSE.EXE
- VSWINPERSE.EXE
- W32DSM89.EXE
- W9X.EXE
- WATCHDOG.EXE
- WEBSCANX.EXE
- WEBTRAP.EXE
- WGFE95.EXE
- WHOSWATCHINGME.EXE
- WIMMUN32.EXE
- WINRECON.EXE
- WNT.EXE
- WRADMIN.EXE
- WrAdmin.EXE
- WRCTRL.EXE
- WrCtrl.EXE
- WSBGATE.EXE
- WYVERNWORKSFIREWALL.EXE
- XPF202EN.EXE
- ZAPRO.EXE
- zapro.EXE
- ZAPSETUP3001.EXE
- ZATUTOR.EXE
- ZAUINST.EXE
- ZONALM2601.EXE
- ZONEALARM.EXE
- zonealarm.EXE
- AVGNT.EXE
- AVGUARD.EXE
- AVWUPSRV.EXE
- \_avp\*
- ackwin32\*
- anti-trojan\*
- aplica32\*
- apvxdwin\*
- autodown\*
- avconsol\*
- ave32\*
- avgcc32\*
- avgctrl\*
- avgw\*
- avkserv\*
- avnt\*
- avp\*
- avsched32\*
- avwin95\*
- avwupd32\*
- blackd\*
- blackice\*
- bootwarn\*
- ccapp\*
- ccshtdwn\*
- cfiadmin\*
- cfiaudit\*
- cfind\*

- cfinet\*
- claw95\*
- dv95\*
- ecengine\*
- efinet32\*
- esafe\*
- eswatch\*
- f-agnt95\*
- findviru\*
- fprot\*
- f-prot\*
- fprot95\*
- f-prot95\*
- fp-win\*
- frw\*
- f-stopw\*
- gibe\*
- iamapp\*
- iamserv\*
- ibman\*
- ibmavsp\*
- icload95\*
- icloadnt\*
- icmon\*
- icmoon\*
- icssuppnt\*
- icsupp\*
- iface\*
- iomon98\*
- jedi\*
- kpfw32\*
- lockdown2000\*
- lookout\*
- luall\*
- moolive\*
- mpftray\*
- msconfig\*
- nai\_vs\_stat\*
- navapw32\*
- navlu32\*
- navnt\*
- navsched\*
- navw\*
- nisum\*
- nmain\*
- normist\*
- nupdate\*
- nupgrade\*
- nvc95\*
- outpost\*
- padmin\*
- pavcl\*
- pavsched\*
- pavw\*
- pcciomon\*

- pccmain\*
- pccwin98\*
- pcfwallicon\*
- persfw\*
- pop3trap\*
- pview\*
- rav\*
- regedit\*
- rescue\*
- safeweb\*
- serv95\*
- sphinx\*
- sweep\*
- tca\*
- tds2\*
- vcleaner\*
- vcontrol\*
- vet32\*
- vet95\*
- vet98\*
- vettray\*
- vscan\*
- vsecomr\*
- vshwin32\*
- vsstat\*
- webtrap\*
- wfindv32\*
- zapro\*
- zonealarm\*
- McVSEscn\*
- mcvsrte\*
- mcvsftsn\*
- mcvsshld\*
- ccapp
- zlclient

4. Microsoft Outlook のアドレス帳及び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。

- .htt
- .htm
- .html
- .hta
- .hte
- .htx
- .shtml
- .stm
- .asp
- .xml
- .doc
- .rtf
- .txt
- .dbx
- .php
- .php3
- .phtml

	<ul style="list-style-type: none"> <li>• .jsp</li> <li>• .sql</li> <li>• .eml</li> </ul> <p>5. Microsoft Outlook の機能を使用して、収集したメールアドレスに自分自身のコピーを送信する。</p> <p>6. MSN Messenger または America Online を使用して、オンラインのコンタクトにメッセージを送信する。なお、受信者が次の URL をクリックすると、W32.Spybot.Worm の亜種が侵入先のコンピュータにダウンロードされ、実行される。</p> <p style="text-align: center;"><a href="http://j0r.biz/[削除]/lolcentral.php?vid0017">http://j0r.biz/[削除]/lolcentral.php?vid0017</a> your pic it's funny lol :P</p> <p>7. hosts ファイルに次のテキストを追加し、複数のセキュリティ関連の Web サイトへのアクセスを遮断する。</p> <ul style="list-style-type: none"> <li>• 127.0.0.1 www.symantec.com</li> <li>• 127.0.0.1 securityresponse.symantec.com</li> <li>• 127.0.0.1 symantec.com</li> <li>• 127.0.0.1 www.sophos.com</li> <li>• 127.0.0.1 sophos.com</li> <li>• 127.0.0.1 www.mcafee.com</li> <li>• 127.0.0.1 mcafee.com</li> <li>• 127.0.0.1 liveupdate.symantecliveupdate.com</li> <li>• 127.0.0.1 www.viruslist.com</li> <li>• 127.0.0.1 viruslist.com</li> <li>• 127.0.0.1 f-secure.com</li> <li>• 127.0.0.1 www.f-secure.com</li> <li>• 127.0.0.1 kaspersky.com</li> <li>• 127.0.0.1 www.avp.com</li> <li>• 127.0.0.1 www.kaspersky.com</li> <li>• 127.0.0.1 avp.com</li> <li>• 127.0.0.1 www.networkassociates.com</li> <li>• 127.0.0.1 networkassociates.com</li> <li>• 127.0.0.1 www.ca.com</li> <li>• 127.0.0.1 ca.com</li> <li>• 127.0.0.1 mast.mcafee.com</li> <li>• 127.0.0.1 my-etrust.com</li> <li>• 127.0.0.1 www.my-etrust.com</li> <li>• 127.0.0.1 www.trendmicro.com</li> <li>• 127.0.0.1 trendmicro.com</li> <li>• 127.0.0.1 download.mcafee.com</li> <li>• 127.0.0.1 dispatch.mcafee.com</li> <li>• 127.0.0.1 secure.nai.com</li> <li>• 127.0.0.1 updates.symantec.com</li> <li>• 127.0.0.1 update.symantec.com</li> </ul>
<b>感染・発症防止方法</b>	<ol style="list-style-type: none"> <li>1. 予期せぬメールが届いた場合には、安易に開封したり、添付ファイルを開かない。特にウイルスの動作概要で記述したようなメールには注意する。</li> <li>2. インターネットからダウンロードしたファイルについては、必ずウイルススキャンを実行し、問題がないことが確認できるまでは絶対に起動しない。</li> </ol>
<b>ウイルスの駆除方法</b>	<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"> <li>1. 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。</li> </ol>

	<ol style="list-style-type: none"><li>2. システムの復元オプションを無効にする。(Windows Me/XP)</li><li>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。</li><li>4. 感染ファイルを削除する。 %System%\windows32.exe</li><li>5. レジストリに行われた変更を元に戻す。 次のレジストリキーから HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 次の値を削除する。 "services" = "%System%\windows32.exe"</li></ol> <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>
<b>その他</b>	平成17年末現在で 8 件(国内 0 件)の届出がシマンテック社に寄せられている。