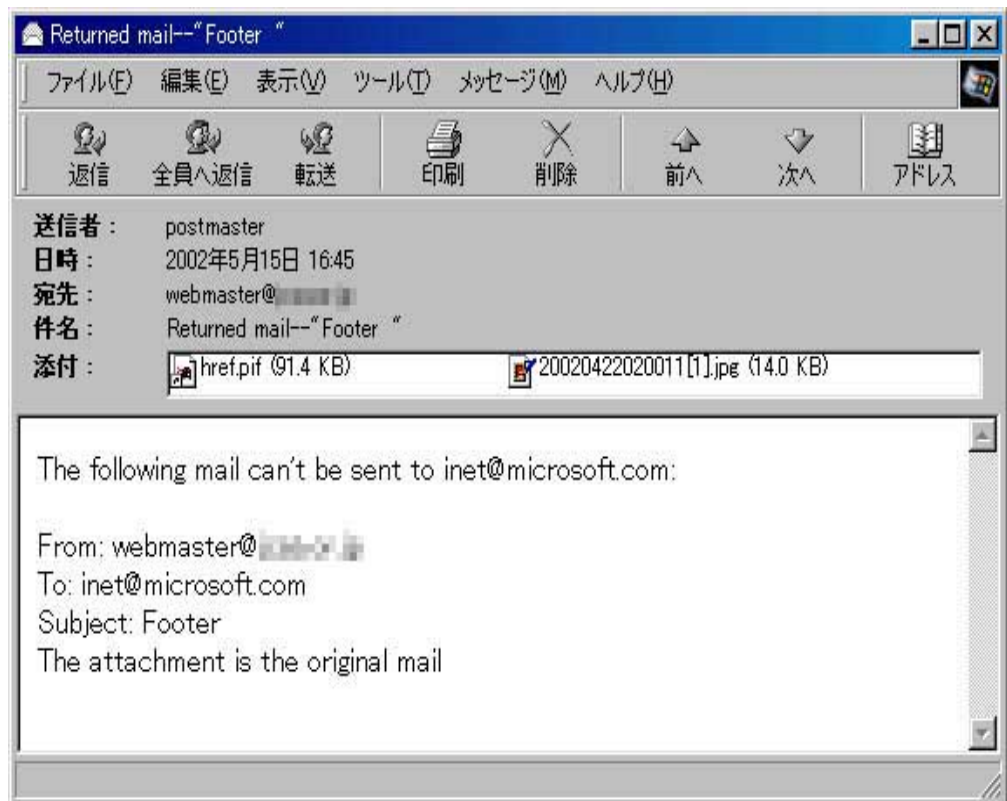


ウィルス解析報告書

ウイルス名	W32/Klez.H
プログラム名及び容量 (添付ファイル名)	名称不定、サイズ約90KB程度、ただし感染コンピュータのSystemフォルダにWINK(2～3桁の数字).EXEという名称でコピーされる。
種別	ウイルス型(狭義ウイルス)
プログラム言語:	32ビットアセンブラ
発症環境	Window95/98/ME/NT/2000/XP(INTEL)
発見日時	2002年4月
発見場所(発信地)	アジア
危険性	感染力が強く、非常に危険 (5段階で4)
発症条件	
ウイルスの活動、影響	ワーム添付メールが発信される。メール送信者を偽って送信されるため、送受信者間で誤解や冤罪が発生する可能性がある。
被害の規模	
亜種、変種の有無	2002年5月時点でA型からH型までの8種類ある。プログラムのにはH型はかなりの変更が見られ、それ以前のタイプとは発病が異なっている。
ウイルス動作概要	<p>このウイルスはWindows95/98/ME/NT/2000/XPで動作する32ビットのワームである。ウイルスは起動すると、ウイルス内部の暗号化されているデータを復号する。</p> <p>ウイルスが既にインストールされているか判別する。 既にインストールされているときには、そのファイルのフルパス、レジストリのキーの名前を取得する。インストールされていないときにはファイルのフルパスとレジストリのキーの名前を作る。 キーは、NT系ならばHKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services以下、95系ならばHKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run以下になる。 キーの名前やファイル名はWink???(???は2～3文字のアルファベット小文字)になる。</p> <p>ウイルスはAPIを動的に取得する。</p> <p>ウイルスはウイルスがまだインストールされていないときには、ウイルス自身を上記で求めたパスにコピーする。リソースのセクションを求める。コピーしたファイルのファイルサイズを変更する。またコピーしたファイルの日時を乱数で改変する。</p> <p>ウイルスはウイルス内部に子プロセスとして起動すべきファイルのパスがあるときには、そのファイルをコピーして子プロセス起動する。子プロセスが終了するまでウイルスは待機する。</p> <p>ウイルスはウイルス自身がインストールされたウイルスとして実行されていないときには終了する。</p> <p>ウイルスはスレッドを作る。このスレッドでは下記の処理が繰り返される。 ウイルスはレジストリの HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services以下を列挙してキーワード(1)を含む記述を削除する。レジストリの HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run およびRunService以下を列挙してキーワード(1)を含む記述を削除する。 プロセスを列挙してキーワード(2)を含むプロセスを終了させる。 そしてそのファイルを削除する。</p> <p>ウイルスはスレッドを作る。このスレッドでは下記の処理が繰り返される。 ウイルスはOutlookExpressのアドレス帳のファイルのパスをレジストリから取得してファイルからメールアドレスを収集する。 ファイルを再帰的に検索して拡張子が.txt、.htm、.htmlのファイルからメールアドレスを収集する。またICQのフォルダにあるファイルからもメールアドレスを収集する。</p>



ウイルスはレジストリの
 HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager\Accounts\
 以下の SMTP ServerおよびSMTP Email Addressからメールサーバとメールアドレスを取得する。

キーワード(1)

_AVP32
 _AVPCC
 NOD32
 NPSSVC
 NRESQ32
 NSCHED32
 NSCHEDNT
 NSPLUGIN
 NAV
 NAVAP SVC
 NAVAPW32
 NAVLU32
 NAVRUNR
 NAVW32
 _AVPM
 ALERTSVC
 AMON
 AVP32
 AVPCC
 AVPM
 N32SCANW
 NAVWNT
 ANTIVIR
 AVPUPD
 AVGCTRL
 AVWIN95
 SCAN32
 VSHWIN32
 F-STOPW
 F-PROT95
 ACKWIN32
 VETTRAY
 VET95
 SWEEP95
 PCCWIN98
 IOMON98

	AVPTC AVE32 AVCONSOL FP-WIN DVP95 F-AGNT95 CLAW95 NVC95 SCAN VIRUS LOCKDOWN2000 Norton Mcafee Antivir TASKMGR キーワード(2) Sircam Nimda CodeRed WQKMM3878 GRIEF3878 Fun Loving Criminal Norton Mcafee Antivir Avconsol F-STOPW F-Secure Sophos virus AVP Monitor AVP Updates InoculatelT PC-cillin Symantec Trend Micro F-PROT NOD32
感染・発症防止方法	<p>Internet Explorer5.0/5.5の不具合である「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」が存在する場合は、Internet Explorer5.0/5.5SP2 (ServicePack2)またはInternet Explorer6.0にアップデートして不具合を解消する。これによってメールやエクスプローラ上でプレビューされた瞬間にワーム感染することを防ぐことができる。</p> <p>メール内容の意図が不鮮明、または心当たりがない場合は、添付ファイルをひらいたり実行したりしない。</p>
ウイルスの駆除方法	<p>< 確認 > NT系ならば、レジストリのHKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services以下、95系ならば、レジストリの HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run以下にファイル名が Wink???(???は2～3文字のアルファベット小文字)があるかどうか確認する。</p> <p>< 駆除 > NT系ならば、レジストリのHKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services以下、95系ならば、レジストリの HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run以下にファイル名が Wink???(???は2～3文字のアルファベット小文字)があればこれを削除する。</p>
その他	報告書作成:2002年6月4日現在

W32/Klez.H ゼネラルフローチャート

