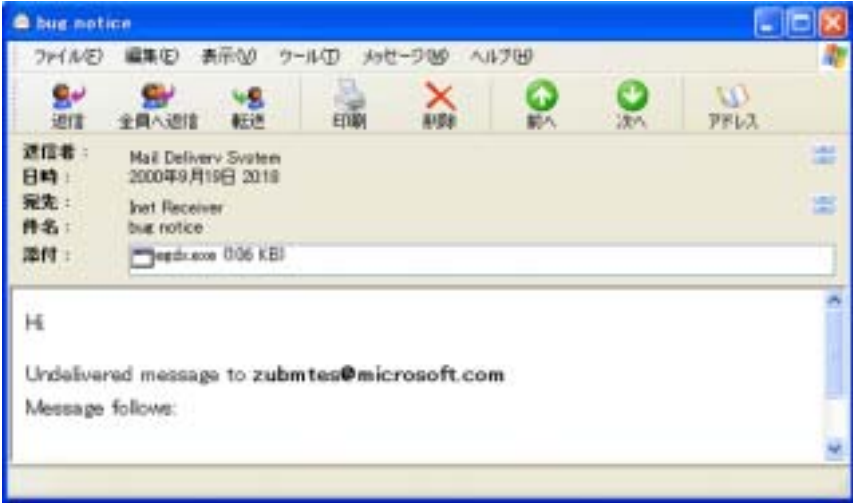
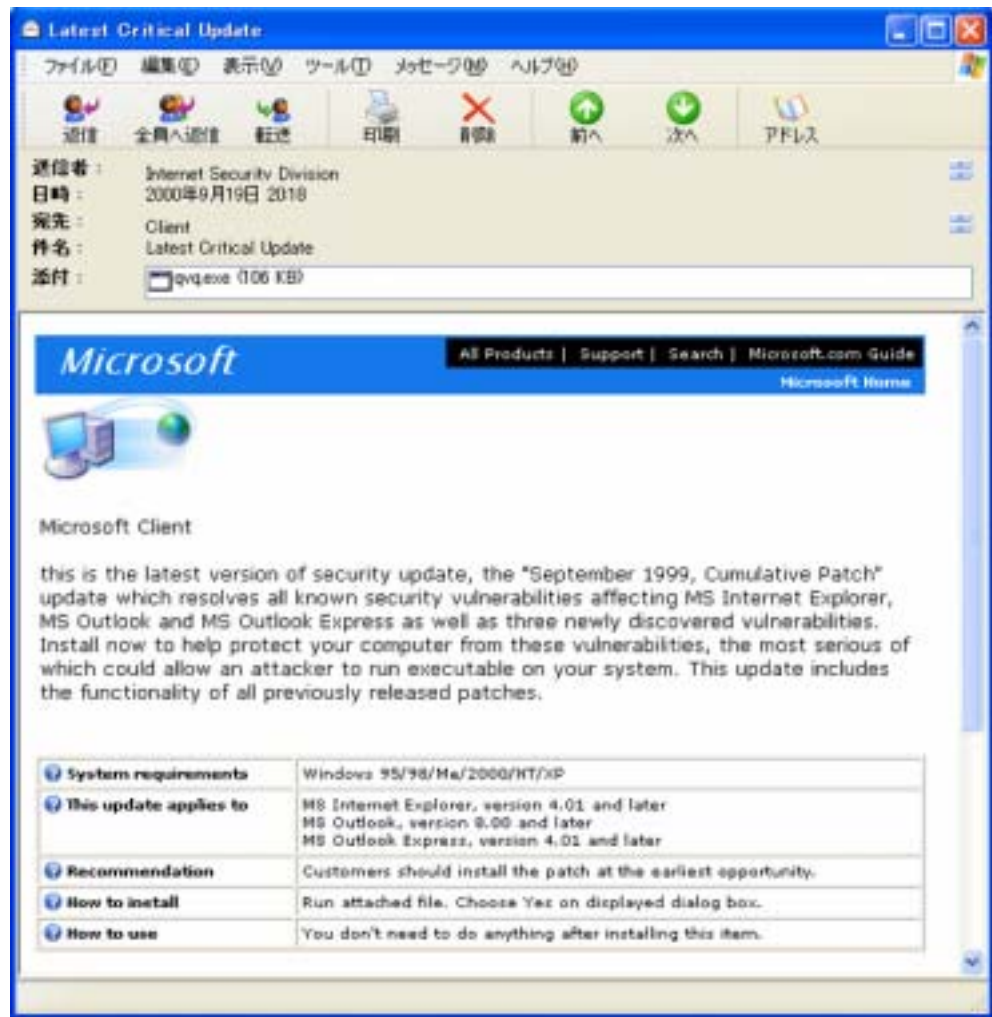


# ウイルス解析報告書

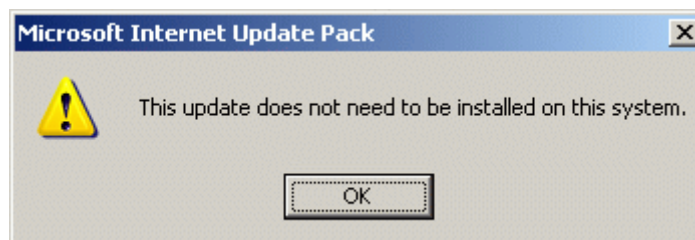
<b>ウイルス名</b>	W32.Swen.A@mm (別名: Swen [F-Secure], W32/Swen@mm [McAfee], W32/Gibe-F [Sophos], Worm Swen.A, Worm.Automat.AHB [Symantec による以前の検出名])
<b>プログラム名及び容量(添付ファイル名)</b>	ランダムなファイル名(106,496 バイト)
<b>種 別</b>	ワーム
<b>プログラム言語</b>	C++
<b>発 症 環 境</b>	Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP
<b>発 見 日 時</b>	2003 年 9 月 19 日
<b>発見場所(発信地)</b>	オランダ(最初の感染報告があった場所)
<b>危 険 性</b>	Microsoft Outlook および Outlook Express の既知であるの脆弱性(不正な MIME ヘッダーの脆弱性: マイクロソフト セキュリティ情報 MS01-020 参照)を利用し、ユーザはメールを閲覧するだけで添付されているワームファイルが自動的に実行されてしまうので危険である。危険度は 5 段階の 3。
<b>発 症 条 件</b>	添付ファイルを実行または脆弱性が存在するコンピュータでは、メールのメッセージを読んだり、メッセージをプレビューした時点で感染する。
<b>ウイルスの活動、影響</b>	W32.Swen.A@mm は、独自の SMTP エンジンを利用して自分自身を拡散する大量メール送信型のワームである。KaZaA や IRC などのファイル共有ネットワークを介して拡散を試みる。また、動作中のセキュリティ対策プログラムを終了させようとする。電子メールの添付ファイルとして届く。メールの件名、本文、差出人欄に表示されるアドレスは不定。Microsoft Internet Explorer の修正プログラムの案内メールを装ったり、qmail からの送信エラー通知メールを装ったりしたものがある。機能面では W32.Gibe.B@mm に似ている。
<b>被 害 規 模</b>	最初の報告から 2003 年 9 月 26 日までに、5962 件(国内は 69 件)の届出がシマンテック社に寄せられている。
<b>変種、亜種の有無</b>	無
<b>ウイルスの動作概要</b>	<p>ワームによって送信されるメールの差出人や本文の内容、添付ファイルなど不特定である。マイクロソフトからの重要なお知らせを装い、ユーザに添付されているファイルを使用してシステムの更新を促すもや、メール送信エラー通知メールを装っているものがある。</p> <p>メール送信エラー通知メールの例</p> 

### マイクロソフト社を装った偽メールの例

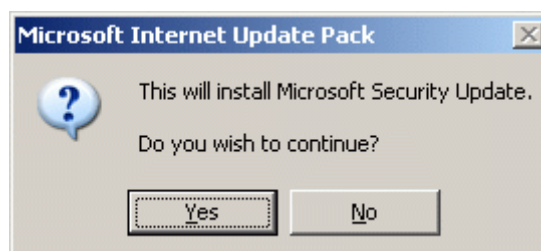


ワームが実行されると次のような動作を行う。

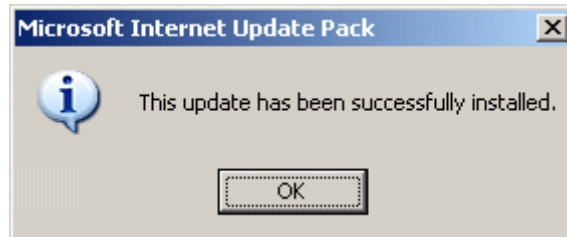
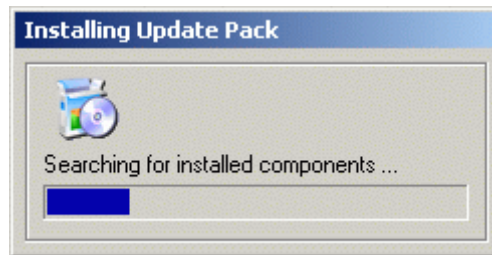
1. ワームが既にインストールされているかどうかをチェックする。インストール済みの場合、インストールプロセスは終了し、次のメッセージを表示する。



2. ファイル名の接頭語が q, u, p, あるいは i ではじまっている場合、ワームは次のダイアログボックスを表示する。



上記ダイアログボックスで「Yes」、「No」のどちらを選択したとしても、インストールは実行される。「No」を選択した場合、ワームはユーザーに分からないようにインストールされる。「Yes」を選択した場合、ワームがインストールされる間、次のダイアログボックスが表示される。



3. 次のプロセスを終了させようとする。これらのプロセスは主にウイルス対策用ソフトなどのセキュリティ関連ソフトである。

- ・ \_avp
- ・ avwupd32
- ・ avwin95
- ・ avsched32
- ・ avp
- ・ avnt
- ・ avkserv
- ・ avgw
- ・ avgctrl
- ・ avgcc32
- ・ ave32
- ・ avconsol
- ・ autodown
- ・ apvxdwin
- ・ aplica32
- ・ anti-trojan
- ・ ackwin32
- ・ bootwarn
- ・ blackice
- ・ blackd
- ・ claw95
- ・ cfinet
- ・ cfind
- ・ cfiaudit
- ・ cfiadmin
- ・ ccshdwn
- ・ ccapp
- ・ dv95
- ・ espwatch
- ・ esafe

- efinet32
- ecengine
- f-stopw
- frw
- fp-win
- f-prot95
- fprot95
- f-prot
- fprot
- findviru
- f-agnt95
- gibe
- iomon98
- iface
- icsupp
- icssupnt
- icmoon
- icmon
- icladnt
- icload95
- ibmavsp
- ibmasn
- iamserv
- iamapp
- jedi
- kpfw32
- luall
- lookout
- lockdown2000
- msconfig
- mpftray
- moolive
- nvc95
- nupgrade
- nupdate
- normist
- nmain
- nisum
- navw
- navsched
- navnt
- navlu32
- navapw32
- nai\_vs\_stat
- outpost
- pview
- pop3trap
- persfw
- pcfwallicon
- pccwin98
- pccmain

- ・ pccimon
- ・ pavw
- ・ pavsched
- ・ pavcl
- ・ padmin
- ・ rescue
- ・ regedit
- ・ rav
- ・ sweep
- ・ sphinx
- ・ serv95
- ・ safeweb
- ・ tds2
- ・ tca
- ・ vsstat
- ・ vshwin32
- ・ vsecomr
- ・ vscan
- ・ vettray
- ・ vet98
- ・ vet95
- ・ vet32
- ・ vcontrol
- ・ vcleaner
- ・ wfindv32
- ・ webtrap
- ・ zapro
- ・ zonealarm

4. 自分自身のコピーを、ランダムなファイル名を使ってWindowsのインストール先フォルダ(標準では C:\Windows または C:\WINNT)以下%Windir%に挿入する。
5. ハードディスク上の .html(.ht\*), .asp, .eml, .dbx, .wab、および .mbx ファイルを検索し、電子メールアドレスを探す。
6. %Windir%\%Germ0.dbv ファイルを作成する。このファイルは、ワームが発見したメールアドレスの保存場所として使用される。
7. %Windir%\%Swen1.dat ファイルを作成する。このファイルは、リモートのニュースサーバーおよびメールサーバーのリストの保存場所として使用される。
8. 感染先のコンピュータ名 %bat ファイルを挿入する。このファイルはワームを実行し、ランダムな名前が付いた設定ファイルを作成し、そのファイルに感染先のコンピュータ固有のデータを保存する。
9. 次の値をレジストリキーに追加する。
  - ・ "CacheBox Outfit"="yes"
  - ・ "ZipName"="<ランダム>"
  - ・ "Email Address"="<ワームがレジストリから探し出した現ユーザーの電子メールアドレス>"
  - ・ "Server"="<ワームがレジストリから探し出した SMTP サーバの IP アドレス>"

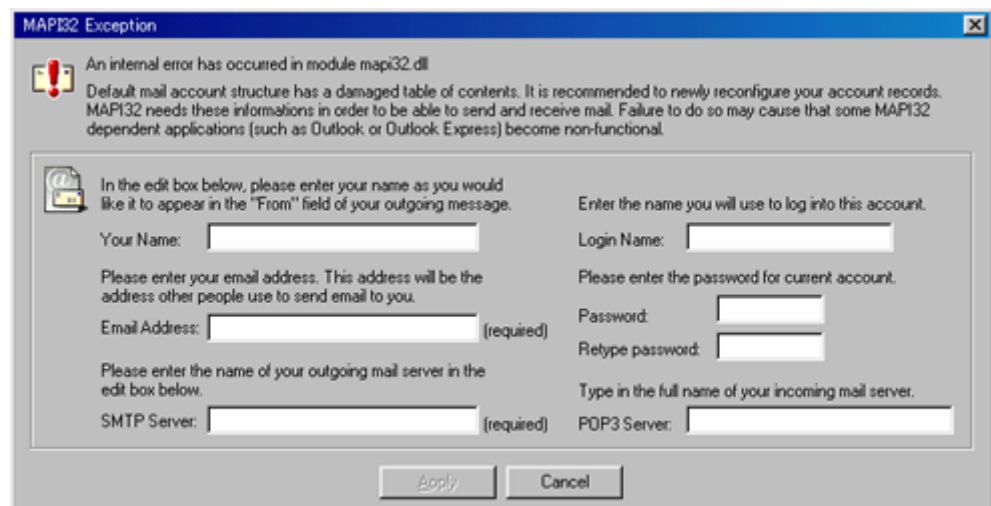
- ・ "Mirc Install Folder"="<mIRC クライアントが格納されている場所>"
- ・ "Installed"="...by Begbie"
- ・ "Install Item"="<ランダム>"
- ・ "Unfile"="<ランダム>"

次のレジストリキーを追加する

HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥explorer¥\*

\* には、ランダムな文字列が入る。

10. ランダムな名前前の値を次のレジストリキーに作成することによって、HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run Windows の起動時に必ずワームが起動するように設定する。
11. 次のレジストリキーを改変し、下記の各ファイルタイプにワームをフックさせる。
- ・ HKEY\_LOCAL\_MACHINE¥CLASSES¥exefile¥shell¥open¥command
  - ・ HKEY\_LOCAL\_MACHINE¥CLASSES¥regfile¥shell¥open¥command
  - ・ HKEY\_LOCAL\_MACHINE¥CLASSES¥scrfile¥shell¥open¥command
  - ・ HKEY\_LOCAL\_MACHINE¥CLASSES¥comfile¥shell¥open¥command
  - ・ HKEY\_LOCAL\_MACHINE¥CLASSES¥batfile¥shell¥open¥command
  - ・ HKEY\_LOCAL\_MACHINE¥CLASSES¥piffile¥shell¥open¥command
12. 次のレジストリキーの値を変更することによって、そのシステム上で、regedit を実行できなくする。
- HKEY\_CURRENT\_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥System の値を以下のように変更する
- "DisableRegistryTools" = "1"
13. 定期的に、次のような偽の MAPI32 例外エラーメッセージを表示し、



ユーザに次の情報を含むメールアカウント情報を入力するように促す。

- ・ 電子メールアドレス
- ・ ユーザ名
- ・ ログイン名
- ・ パスワード
- ・ POP3 サーバー
- ・ SMTP サーバー

14. ユーザー名とパスワードを利用することで、ワームは、POP3 サーバにログインし、ユーザーの

電子メールをチェックする。ワームが送信した電子メールを見つけた場合、そのメールは削除される。ワームは、現在の感染コンピュータから送信されたメッセージのみを削除する。

15. ステップ3にリストされているあらゆるプロセスの実行を妨害し、それらがロードされることを防ぐ。そして、ユーザーに次の偽装メッセージを表示する。



16. ワームが初めて実行される際、カウンター情報を探す目的で、予め定義された HTTP サーバに対し HTTP Get リクエストを送る。ワームは、カウンター情報を表示することがある。

**831407**

17. 自分自身を圧縮した複製(1 つ以上)を、Winzip や Winrar などの 圧縮ツールを利用して作成する。

### ワームの感染形態

1. 電子メールによる感染拡大

様々な方法を使用してシステム上で発見したメールアドレスに自分自身のコピーを送信する。このワームが送信するメールの内容や添付ファイルの名前は不特定である。このワームは不正な MIME ヘッダーの脆弱性(マイクロソフト セキュリティ情報 MS01-020 参照)を利用するため、ユーザはメールを閲覧するだけで添付されているワームファイル(拡張子は、.exe あるいは .zip)が自動的に実行されてしまう。

送信されるメールの中には、マイクロソフトからの重要なお知らせを装い、ユーザに添付されているファイルを使用してシステムの更新を促すものがある。

また、差出人を詐称したメール送信エラーの通知メールを送信することもある。そのメールには、ワームがランダムな名前の実行形式ファイルとして添付されている。以下はこの種のメール本文の一例である。

```
" This is the qmail program
I'm sorry to haveto inform you that the message returned
Below could not bedelivered to the following addresses;
```

```
Undeliverd mail to hinzagdwp@freemail.com      "
```

"I'm sorry I wasn't able to deliver your message to one or more destinations." 等

2. KaZaA を介した感染拡大

KaZaA を介して感染拡大を試みる際、次のことを行う。

- (1) 感染しているシステム上の%Temp%フォルダにランダムな名前のサブフォルダ<random folder name>を作成し、その場所に自分自身のコピーを挿入する。( %Temp% は可変。このワームは Windows のインストール先フォルダを探し出し、その場所に自分自身をコピーする。)

- (2) レジストリキー HKEY\_CURRENT\_USER¥Software¥Kazaa¥LocalContent に次の値を追加する

```
"Dir99"= 012345:"<random folder name>"
```

"DisableSharing"="0"

そのフォルダ<random folder name>を、KaZaA の共有フォルダリストに追加する。

(3) %Temp%フォルダに作成したフォルダ<random folder name>に自分自身を様々な名前のファイルとしてコピーする。そのとき使用されるファイル名の一例。

- ・ Virus Generator
- ・ Magic Mushrooms Growing
- ・ Cooking with Cannabis
- ・ Hallucinogenic Screensaver
- ・ My naked sister
- ・ XXX Pictures
- ・ Sick Joke
- ・ XXX Video
- ・ XP update
- ・ Emulator PS2
- ・ XboX Emulator
- ・ Sex
- ・ HardPom
- ・ Jenna Jameson
- ・ 10.000 Serials
- ・ Hotmail hacker
- ・ Yahoo hacker
- ・ AOL hacker
- ・ Fixtool
- ・ Cleaner
- ・ removal tool
- ・ remover
- ・ Klez
- ・ Sobig
- ・ Sircam
- ・ Gibe
- ・ Yaha
- ・ Bugbear
- ・ installer
- ・ upload
- ・ warez
- ・ Hacked
- ・ Hack
- ・ key generator
- ・ Windows Media Player
- ・ GetRight FTP
- ・ Download Accelerator
- ・ Mirc
- ・ Winamp
- ・ WinZip
- ・ WinRar
- ・ KaZaA
- ・ KaZaA media desktop
- ・ Kazaa Lite

3. IRC を介した感染拡大

IRC を介して感染拡大を試みる際、次のことを行う。

	<p>(1) %Mirc フォルダを探す。</p> <p>(2) そのフォルダに、Script.ini ファイルを作成する。ワームはその Script.ini ファイルを使って、感染先のコンピュータと同じチャンネルに接続した他の mIRC ユーザに自分自身を送信する。</p> <p><b>4. マッピングされているネットワークドライブを通じた感染拡大</b></p> <p>マッピングされたドライブを通じて感染拡大を試みる際に次の場所を見つけコピーしようとする。</p> <ul style="list-style-type: none"> <li>・ %Win98%Start menu%Programs%Startup</li> <li>・ %Win95%Start menu%Programs%Startup</li> <li>・ %WinMe%Start menu%Programs%Startup</li> <li>・ %Windows%Start menu%Programs%Startup</li> <li>・ %Documents and Settings%All Users%Start menu%Programs%Startup</li> <li>・ %Documents and Settings%Administrator%Start menu%Programs%Startup</li> <li>・ %Documents and Settings%Default User%Start menu%Programs%Startup</li> <li>・ %Winnt%Profiles%All Users%Start menu%Programs%Startup</li> <li>・ %Winnt%Profiles%Administrator%Start menu%Programs%Startup</li> <li>・ %Winnt%Profiles%Default User%Start menu%Programs%Startup</li> </ul> <p><b>5. ニュースグループを介した感染拡大</b></p> <ul style="list-style-type: none"> <li>・ ニュースグループサーバのアドレスをレジストリから調べ、自分自身を送信しようとする。</li> <li>・ ニュースグループサーバの情報がシステム上に無い場合、事前に定義されたリストからランダムにサーバを選択する。</li> <li>・ ランダムに選択したグループから、利用可能なグループをダウンロードし、メッセージをポストする。</li> <li>・ ニュースグループにポストするメッセージは、メールを送信する方法と同じ要領で行う。</li> </ul>
<p><b>感染・発症防止方法</b></p>	<p>1.ワームは、Microsoft Outlook、および Outlook Express の脆弱性を悪用し、メッセージを読んだり、メッセージをプレビューで開いたとき自分自身を実行する。これは修正パッチを適用することで回避することができる。この脆弱性に関する情報、および修正パッチは、マイクロソフト社の Web サイト(マイクロソフト セキュリティ情報 MS01-020 参照)を参照。</p> <p>2. 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。</p> <p>3. 特に拡張子が zip、.exe が付いたメールは安易に開封しない。</p>
<p><b>ウイルスの駆除方法</b></p>	<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がある。</p> <p>W32.Swen.A@mm は、自分自身をランダムなファイル名を使ってコピーするので感染ファイルを特定するのが難しく、手動による修復は非常に困難である。</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>
<p><b>その他</b></p>	<p>なし</p>