

VIRUS ANALYSIS

WHO? WHAT? WHERE? SWEN?

Peter Ferrie

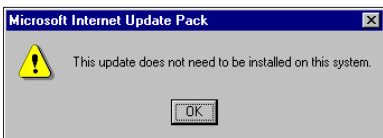
Symantec Security Response, USA

W32/Swen spreads in email and newsgroups, across network shares, through peer-to-peer networks, and on IRC. It contains a reasonably authentic-looking message purporting to come from *Microsoft*, and another message that uses an exploit. It hooks file extensions in the registry, and terminates anti-virus and firewall software. Something for everyone, one might say.

INSTALLATION

Whenever W32/Swen is run, it examines its command line. If the command line is empty (which is the case when it is run from an email attachment), the virus will look for its infection marker in the registry.

The infection marker is located in 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer' and consists of a string of pseudo-random upper-case letters, the sum of whose positions in the alphabet (i.e. A=1, B=2, C=3, etc.) is 80. If the infection marker is not found, the virus creates one by constructing a string of random upper-case letters, until the sum of the letters' positions in the alphabet exceeds 53. At this point, the virus adds one more upper-case letter whose position in the alphabet will produce the required sum of 80.



If the infection marker contains a value called 'Installed' whose data are set to '... by

Begbie', regardless of the letter case, and if the filename used to run the virus begins with the letter 'p', 'q', 'u', or 'i' – again regardless of case – the virus displays a message which states that 'the update' does not need to be installed on this system.

Otherwise, the virus copies itself to the %windir% directory using a filename of between four and eight random lower-case letters with '.exe' appended. Then it creates the 'HKLM\Software\Microsoft\Windows\CurrentVersion\Run' key in the registry, using a value of four to nine random lower-case letters, whose data are set to the name of the file copied to the %windir% directory. This allows the virus to run whenever *Windows* is started. In order to avoid running this code every time the virus is run, the 'autorun' parameter is added to the registry value data. The virus writes this 'Run' value to a value called 'Install Item' in the infection marker registry key. If the filename used to run the virus



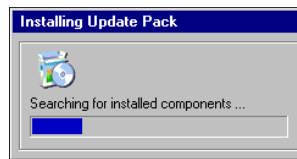
begins with 'p', 'q', 'u', or 'i' (regardless of case), the virus displays a prompt to install a Microsoft Security Update.

The virus will install itself regardless of what the user selects at this prompt, the only difference being that if the user selects 'Yes', the virus will display a dialog box showing its progress.

UNDO THE DEED

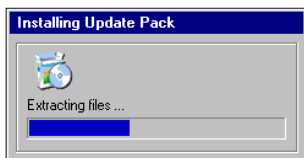
If the name of the computer can be retrieved by the GetComputerNameA() API, the virus will create the files necessary to allow the removal of the virus. First, it creates a file called '%windir%\%computername%.bat', which contains code to run the virus, passing the exact pathname of the virus as the first parameter, and a user-specified parameter as the second.

Next, the virus checks for the existence of a value called 'Unfile' in the infection marker registry key. If this value does not exist, the virus writes to the registry key a string of between four and eight random lower-case letters, followed by '.', followed by three random lower-case letters, and creates the 'Unfile' file in the %windir% directory. The virus updates this 'Unfile' file by appending '%windir%\%computername%.bat'. It is not a bug for the virus to append continually to this file – since it is used for uninstallation, it contains the names of all installed components, thus all files ever created, including those created by partial installations, must be listed.



If the user answered 'Yes' to install the 'update', the virus displays a message, stating that it is searching for installed components.

Now the virus searches for email addresses. The search is conducted recursively in all subdirectories on all hard disks, for files whose extension contains anywhere within it the letters 'ht' or 'asp', and whose filesize is at least 50 bytes; or whose extension is 'mbx', 'dbx', 'wab', or 'eml', and whose filesize exceeds 100 bytes. The virus searches for email addresses within each such file that is found. The contents of files whose extension contains 'ht' and 'asp' are searched for the 'mailto:' string. The other files are searched blindly for text that resembles email addresses. Duplicate email addresses are not added to the list. On completion of the search, and if email addresses have been found, the virus creates a file called '%windir%\germs0.dbv' (if it does not exist already), and appends each address to the file. Once the search has completed, the virus writes 'Yes' to a



value called 'CacheBox Outfit' in the infection marker registry key.

If the user answered 'Yes' to install the 'update', the

virus displays a message which indicates that it is extracting files.

EXTRACTING FILES

Despite what the dialog box says, no files are extracted by the virus. In fact, the opposite is the case. The virus copies itself to the %temp% directory, using a filename chosen randomly from one of the following possibilities:

- the letter 'q', followed by either six random numbers or one to four random lower-case letters
- the word 'patch' or 'pack', which may be followed by two to four random numbers
- the word 'update' or 'upgrade', which may be followed by two to four random numbers
- the word 'install', 'installation', or 'installer', which may be followed by two to four random numbers

A 'feature' of the code that produces the strings of random numbers is that it never produces a string that contains '0'. Additionally, the case of the first letter can be altered individually, or the entire string can be converted to upper-case, however the suffix of the filename is always '.exe', regardless of the letter-case of the rest of the string.

After the virus has copied itself to the %temp% directory, it constructs an archive filename of between four and eight random lower-case characters followed by '.zip', and attempts to compress the original file, using *WinRAR* or *WinZip*. The virus attempts to run *WinRAR* first, relying on the *Windows* default search path. If that fails, the virus queries the registry for the 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\WinRAR.exe' value. If this value exists, the virus tries to run *WinRAR* from the directory specified in the value data. If this is unsuccessful, the virus attempts to run *WinZip* – first from the *Windows* default search path, then by querying the registry for the 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\WinZip.exe' value. However a bug exists in this code – the command-line that is passed to *WinZip* is incorrect, and an error will be displayed.

If the archiving is successful, the virus writes the archive filename to a value called 'ZipName' in the infection marker registry key, and updates the 'Unfile' file by appending the archive pathname. The virus then deletes the .exe file from the %temp% directory.

THE DANGERS OF FILE SHARING

If the 'HKCU\Software\Kazaa' registry key exists in the registry, the virus enables file sharing by writing a 0 to the registry value 'HKCU\Software\Kazaa\LocalContent\DisableSharing'. The virus is aware of the different versions of the *KaZaA* file-sharing software, and queries the registry for the 'HKCU\Software\Kazaa\LocalContent\DownloadDir' and 'HKCU\Software\Kazaa\Transfer\Dir0' values. If either of these exists, the virus will create a number of filenames aimed at enticing people to download them. These are chosen randomly from the following options:

1. One of:

AOL hacker	XP update
Yahoo hacker	XXX Video
Hotmail hacker	Sick Joke
10.000 Serials	XXX Pictures
Jenna Jameson	My naked sister
HardPorn	Hallucinogenic Screensaver
Sex	Cooking with Cannabis
XboX Emulator	Magic Mushrooms
Emulator PS2	Virus Generator

2. One of:

Bugbear	Sircam	Yaha
Sobig	Gibe	Klez

followed by 'remover', 'cleaner', 'removal tool' or 'fixtool'.

3. One of:

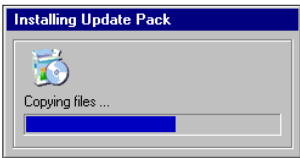
Kazaa Lite	Winamp
KaZaA media desktop	Mirc
KaZaA	Download Accelerator
WinRar	GetRight FTP
WinZip	Windows Media Player

followed by 'key generator', 'warez', 'hack', 'upload', 'hacked' or 'installer'.

The filename may be converted to entirely lower-case letters. If archiving was successful, the virus constructs three to seven of these names, appends '.zip', and copies the archived file to these filenames. If archiving was not successful, the virus constructs only one to three of these names, appends '.exe' and copies the original .exe file to these filenames. In either case, the virus appends these filenames to the 'Unfile' file.

The virus also creates a directory in the %temp% directory, using a string of three to seven random lower-case letters, and writes '012345:%temp%\{directory name}' to the 'HKCU\Software\Kazaa\LocalContent\Dir99' registry value. After creating the directory, the virus creates more

.zip or .exe files in this directory, in the same way as described above. The virus completes the *KaZaA* routine by writing 'Yes' to a value called 'Kazaa Infect' in the infection marker registry key.



If the user answered 'Yes' to install the 'update', the virus displays a message which indicates that it is copying files.

COPYING FILES (1)

If 'mirc.ini' exists in the 'c:\mirc' or 'c:\mirc32' directories, Swen creates another filename, using the same routine as for the *KaZaA* routine, copies itself to the %windir% directory using this new filename, and appends the filename to the 'Unfile' file. If 'script.ini' exists in the mIRC directory, the virus moves it to 'script.bcp', then creates a new 'script.ini' file that contains code that will send the file whenever a user joins a channel shared by the infected user.

The virus writes the name of the mIRC directory to a value called 'Mirc Install Folder' in the infection marker registry key. The virus also queries the registry for the 'HKLM\Software\Microsoft\Windows\CurrentVersion\ProgramFilesDir' value, and looks within the directory listed there for the 'mirc' and 'mirc32' directories. If either of these exists, the virus places a script.ini file in the directory, and updates the 'Mirc Install Folder' value. This is a bug, since only the last mIRC location is saved in the registry, instead of relying on the 'Unfile' file, meaning that some script.ini files remain if the automatic removal is used on machines with multiple copies of mIRC installed.

At this point, the virus queries the registry for the 'HKCU\SOFTWARE\Microsoft\Internet Account Manager\Default Mail Account' value. Its data are used if they exist, otherwise the virus will default to '00000001'. These data are used to retrieve the SMTP information (SMTP Email Address, SMTP Server, SMTP Display Name) from the registry, by querying the 'HKCU\SOFTWARE\Microsoft\Internet Account Manager\Accounts\{mail account}' registry key.

If the retrieved email address appears to be valid, the virus writes it to a value called 'Email Address' in the infection marker registry key, and writes the SMTP server name to a value called 'Server' in the infection marker registry key. If the SMTP Display Name cannot be retrieved, the virus will attempt to retrieve the computer name. If the computer name cannot be retrieved, the virus will use the word 'unknown'. The virus will write the computer name (or 'unknown') to a value called 'VicName' in the infection marker registry key.

The virus queries the registry for the 'HKCU\SOFTWARE\Microsoft\Internet Account Manager\Default News Account' value. If it exists, the virus retrieves the NNTP Server name from the registry by querying the 'HKCU\SOFTWARE\Microsoft\Internet Account Manager\Accounts\{default news account}' registry key. If the server name appears to be valid, the virus writes it to a file called '%windir%\swen0.dat'.

If the user answered 'Yes' to install the 'update', the virus displays the 'Copying files' message again.

COPYING FILES (2)

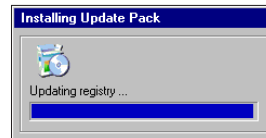
The logic in the virus appears to be confused here, since it does not copy files at this time, but does alter the registry, then displays a message referring to registry alterations before resuming file copying.

The virus carries a list of public news servers in a compressed form. The virus extracts the compressed list to a file called '%temp%\nntptmp.fl', decompresses it, writes the decompressed list to a file called '%windir%\swen1.dat', then deletes the compressed file.

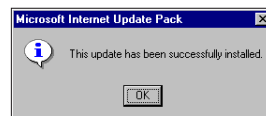
The virus author seems to consider the installation to be complete now – the virus writes '... by Begbie' to a value called 'Installed' in the infection marker registry key, then runs another copy of itself with the 'autorun' parameter.

Meanwhile, the virus hooks the 'HKCR\...\shell\open\command' registry keys for 'exefile', 'comfile', 'piffile', 'batfile', 'scrfile', and 'regfile', and the 'scrfile\shell\config\command'. The virus is aware of the additional parameter for .scr files. For all but the 'regfile' entry, the effect of the change is that the virus examines the file that was requested to run, and possibly runs it.

For the 'regfile' entry, the virus is run with the 'showerror' option instead. The virus also prevents the use of RegEdit and similar applications in *Windows 2000/XP/2003*, by writing a 1 to the 'HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools' registry value.



If the user answered 'Yes' to install the 'update', the virus displays a message that it is updating the registry. However, the virus replaces this message immediately with a message stating that this update has been installed successfully.



ARE WE THERE YET?

Despite what the message says, the installation has not yet

completed. At this point, the virus queries the 'HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Startup' registry value, then attempts to guess the startup directory on network drives. It tries 'Windows', 'WinMe', 'Win95', 'Win98', and each of the following:

- 'All Users\Start menu\Programs\Startup'
- '\Start menu\Programs\Startup'
- {startup value from the registry} if it is different from above

If a directory is found, the virus creates a filename using a string of five to ten random lower-case letters, with '.exe' appended. The virus replaces the first character with a letter from 'a' to 'v' only (perhaps to reduce suspicion), then copies itself to the directory using the new filename.

The virus also looks on network drives for a directory called 'Documents and Settings' or 'Winnt\Profiles', and tries each of the following possibilities:

- 'All Users\Start menu\Programs\Startup'
- 'All Users\{startup value from the registry}'
- 'Default User\Start menu\Programs\Startup'
- 'Default User\{startup value from the registry}'
- 'Administrator\Start menu\Programs\Startup'
- 'Administrator\{startup value from the registry}'

If a directory is found, the virus creates a filename using a string of five to ten random lower-case letters, with '.exe' appended. It does not replace the first character in this case, before it copies itself to the directory using the new filename.

If the virus is run with the 'showerror' parameter (which occurs when the user attempts to run a '.reg' file to restore the registry), the virus displays a fake error message describing an illegal memory access at a certain location. The numbers are chosen randomly by the virus.

NOT WHAT YOU WERE EXPECTING

If the virus is run with a parameter other than 'autorun', Swen will examine the first and second parameters. If either of these contains anywhere within it any one of a long list of anti-virus and firewall applications, the virus will display the message box as though it were run with the 'showerror' parameter.

The checking of the second parameter (if it exists) allows the virus to detect an application that runs any specified application, since that is one way to bypass malware that changes the 'shell\open\command' registry values. If neither of the parameters contains any of those strings, the virus attempts to retrieve the 'OriginalFilename' field from the

version information data in the specified file. This allows the virus to detect renamed files. If the 'OriginalFilename' field contains any of the strings, the virus will also display the 'showerror' message box. It is interesting that 'Gibe' exists in the list: this check works as an inoculation against the W32/Gibe virus ('Begbie' is understood to be the author of both worms).

If the first parameter is the exact pathname of the virus file, and the second parameter is the word 'cure' (regardless of case), the virus will remove itself. This situation can be achieved by running the '%windir%\%computername%.bat' file with the 'cure' parameter.

Removal is performed by terminating any other running copies of the virus, and deleting 'germs0.dbv', 'germs1.dbv', 'swen0.dat', 'swen1.dat' and 'nntpgroups.dat'. The removal code disables file sharing by writing a 1 to the 'HKCU\Software\Kazaa\LocalContent\DisableSharing' registry value, and enables registry tools by writing a 0 to the 'HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools' registry value.

Otherwise, if the first parameter is not recognised, the virus will run the specified file.

A WINDOW ON THE WORLD

The virus uses a window called 'Explorer XBaseBar' to prevent multiple copies of itself running at the same time. If this window does not exist, the virus creates it now and then creates two routines that run periodically.

The first (email) routine is run once every 20 seconds if the SMTP information was able to be retrieved from the registry; otherwise it is run once every two minutes. The virus runs the second (anti-anti-virus) routine now, and every 45 seconds hereafter.

After running the anti-AV routine for the first time, the virus hides itself from the task list on *Windows 9x/Me*, using the RegisterServiceProcess() API, then runs the email routine if the SMTP server name was retrieved successfully. At this point, the virus enters its message loop, waiting for the request to exit.

The anti-AV routine enumerates all processes, looking for process names that contain anywhere within them any strings from the list of anti-virus and firewall names that the virus carries. For each process with a matching name, the virus saves the process ID for later use.

On completion of the enumeration, the virus examines the process ID of each window that exists, and whenever a match is found, the virus sends a request to that window to exit the application. If the request is ignored, the virus terminates the process forcibly.

The virus then checks for the presence of a debugger, using the `IsDebuggerPresent()` API. If a debugger is found, the virus displays another message.

EMAIL ROUTINE

If no email addresses could be found, the virus will call the routine that searches for email addresses described above. If the search was successful but the SMTP information was not retrieved from the registry, the virus will display a fake error dialog, prompting the user to enter email information.

If the user enters this information, the virus will write it to the registry, then write a string of 11–25 random numbers to a value called 'X-ID' in the infection marker registry key. The 'X-ID' value is added to the emails that the virus sends, which allows the virus to identify its own messages. This ability is exploited by the POP3 routine described below. If the SMTP information exists in the registry, the virus will run the email routine once every 20 seconds.

If email addresses were found, the SMTP information exists in the registry, and an active Internet connection exists, the virus checks whether it has visited a website that (used to) keep track of the (approximate) number of infected machines. If such a visit has not occurred, the virus connects to 'ww2.fce.vutbr.cz', and sends sends 'GET http://ww2.fce.vutbr.cz/bin/counter.gif/link=bacillus&width=6&set=cnt006 HTTP/1.0'. If the server returns without error, the virus writes 'yes' to the 'Counter Visited' value in the infection marker registry key.

If the 'X-ID' value exists in the registry, then once in every 20 times that the email routine is run, the virus connects to the specified POP3 server, examines each message in the mail box, and deletes any message that contains the 'X-ID' text, since it is assumed to be a message sent by the virus.

If the '%windir%\germs0.dbv' file does not exist, the virus will switch to the '%windir%\germs1.dbv' file. If the file can be opened, the virus will read the last 51–80 addresses, the exact number is chosen randomly by the virus. The virus then deletes these from the file. If the file is empty, the virus deletes the file.

Using these addresses, the virus connects to the SMTP server, sends 'HELO' followed by a string of four to eight random lower-case letters, sends 'MAIL FROM' followed by the infected user's email address, then sends a 'RCPT TO' line for each address. Thus, a single mail will be sent, but it will have multiple recipients.

The virus sends the email message at this point, but its content depends on which of the 'germs' files is in use. If the file in use is 'germs0.dbv', the virus will produce the following:

The 'FROM' address may begin with 'MS' or 'Microsoft', and may be followed by 'Corporation'. This is always followed by either:

1. 'Network', 'Internet' or 'Program', followed by the word 'Security', followed by 'Center', 'Section', 'Department' or 'Division'.

or

2. 'Customer', 'Technical', 'Public' or 'Security', followed by 'Support', 'Services', 'Assistance' or 'Bulletin'.

The virus can also choose randomly to replace this part of the address entirely with 'Microsoft' or leave it blank. The address continues with 6–15 random lower-case letters, which can optionally be followed by '-' or '_', followed by four to eight random lower-case letters. Then comes the '@', followed by: 'newsletters', 'advisor', 'support', 'confidence', 'technet', 'bulletin', 'updates' or 'news', which can be followed by '_' or '.', followed by 'msdn', 'ms', 'microsoft' or 'msn'. The address always ends with '.net' or '.com'. The virus can also choose randomly to make this part of the address blank.

The virus can choose randomly to make the 'TO' address begin with none or one of 'Microsoft' or 'MS', which may be followed by 'Corporation' or 'Commercial'. This is always followed by 'Client', 'User', 'Consumer', 'Customer' or 'Partner'. The virus can choose randomly to make this part of the address blank.

The address continues with four to nine random lower-case letters or a word from the list beginning with 'Client' above. This may be followed by '.', '_', or '-', followed by 6–11 random lower-case letters. Then comes the '@', followed by the same text that was produced after the previous '@'. The virus can choose randomly to make this part of the address blank.

The virus can choose randomly to begin the 'SUBJECT' line with none or one of: 'Latest', 'Newest', 'New', 'Current', or 'Last'. This may be followed by one of: 'Internet', 'Network', 'Microsoft' or 'Net'. This can optionally be followed by 'Security' or 'Critical', followed by 'Upgrade', 'Update', 'Pack' or 'Patch'.

The virus may choose randomly to convert the subject to entirely lower-case, or leave it blank. If the 'X-ID' value exists in the registry, the virus will add it to the email at this time.

Next the virus assembles the text for the body of the message. It begins with 'MS' or 'Microsoft', followed by a word from the list beginning with 'Client' above. It continues with

```
this is the latest version of security update, the
[month, year], Cumulative Patch update which
```

and follows this with 'eliminates', 'resolves' or 'fixes', and continues with

```
all known security vulnerabilities affecting MS
Internet Explorer, MS Outlook and MS Outlook Express.
```

This can be optionally followed by

```
as well as three new vulnerabilities
```

or

```
as well as three newly discovered vulnerabilities
```

It is always followed by 'Install now to', followed by one of the following three options:

```
help maintain the security of your computer
help protect your computer
continue keeping your computer secure
```

This is followed by 'from these vulnerabilities', which may be followed by 'the most serious of which could allow an', followed by 'malicious user' or 'attacker', followed by 'to run', followed by 'code' or 'executable', followed by 'on your', followed by 'computer' or 'system'.

This may be followed by

```
This update includes the functionality of all
previously released patches
```

This can optionally be followed by the text:

```
System requirements: Windows 95/98/Me/2000/NT/XP
This update applies to:
- MS Internet Explorer, version 4.01 and later
- MS Outlook, version 8.00 and later
- MS Outlook Express, version 4.01 and later
Recommendation: Customers should install the patch at
the earliest opportunity.
How to install: Run attached file. Choose Yes on
displayed dialog box.
How to use: You don't need to do anything after
installing this item
```

This may be followed by

```
Microsoft Product Support Services and Knowledge Base
articles can be found on the Microsoft Technical
Support web site.
http://support.microsoft.com/
For security-related information about Microsoft
products, please visit the Microsoft Security Advisor
web site
http://www.microsoft.com/security/
Thank you for using Microsoft products.
Please do not reply to this message.
It was sent from an unmonitored email address and we
are unable to respond to any replies.
```

```
The names of the actual companies and products
mentioned herein are the trademarks of their respec-
tive owners.
```

This may be followed by

```
Copyright [year] Microsoft Corporation
```

If the file is 'germs1.dbv', the 'FROM' address will be one of the following possibilities:

1. 'MS' or 'Microsoft', which may be followed by 'Internet', 'Net', 'Network' or 'Inet'. This may be followed by 'Mail', 'Message' or 'Email'. This may be followed by 'Delivery' or 'Storage'. This is always followed by 'System' or 'Service'.
2. 'Postmaster', 'Administrator', or 'Admin'.

The virus can choose randomly to convert the address to entirely lower-case, or make it blank.

After this the 'FROM' address continues with 'post', 'email', 'mail', 'mailer', 'web', 'master', 'smtp' or '[random letter]mail', followed by 'service', 'daemon', 'form', 'program', 'engine', 'routine', 'automat', 'bot', or 'robot'. Then comes the '@', followed by 'rocketmail', 'freemail', 'microsoft', 'netmail', 'bigfoot', 'america', 'aol', 'puremail' or 'yahoo'. The address always ends with '.net' or '.com'. The virus can also choose randomly to make this part of the address blank.

The 'TO' address will begin with 'Network', 'Inet', 'Internet', 'Mail', 'Net', or 'Email', followed by 'User', 'Recipient', 'Receiver', or 'Client'. Once again, the virus can also choose randomly to make this part of the address blank.

The address continues with 'user', 'recipient', 'receiver', or 'client', followed by 'home', 'mail', 'mx', 'smtp', 'your' or 'email', followed by 'domain' or 'server'. The address always ends with '.net' or '.com'. The virus can also choose randomly to make this part of the address blank.

The virus can choose randomly to begin the 'SUBJECT' line with one of the following options:

1. 'Failure', 'Error', 'Abort', or 'Bug', followed by 'Notice', 'Message', 'Report', 'Advice', 'Announcement', or 'Letter'.
2. 'Undelivered', 'Undeliverable' or 'Returned', followed by 'Message' or 'Mail', sometimes followed by ':'. This is always followed by 'User unknown', 'Mailer', or 'Sender'.

The virus can choose randomly to convert the address to entirely lower-case, or make it blank. If the 'X-ID' value exists in the registry, the virus will add it to the email at this time.

Next the virus assembles the text for the body of the message. The text may begin with 'Hi.', and may be followed by

```
This is the qmail program
```

or

```
Message from [from: address, as above]
```

This may be followed by one of

```
I'm afraid
I'm sorry to have to inform you that
I'm sorry
```

This is always followed by one of

```
the message returned below could not be delivered
```

or

```
I wasn't able to deliver your message
```

and followed by one of

```
to one or more destinations.
to the following addresses:
```

This is followed by 'Undelivered' or 'Undeliverable', and may be followed by 'mail' or 'message'. This is followed by

```
to [6-11 random lower-case letters]@[word from list
that begins with "rocketmail"]
```

This may be followed by 'Message follows:'. The virus uses the [MS01-020 exploit], randomly choosing 'x-wav' or 'x-midi' as the MIME Content-Type. The file extension is chosen randomly from: 'com', 'scr', 'bat', 'pif' and 'exe'.

In either case, the virus attaches itself to the email and sends the message now. After sending the message, the virus writes the used addresses to the '%windir%\germs1.dbv' file. There is another bug in the virus here: when the 'germs0.dbv' file is exhausted, the last 51–80 entries in the 'germs1.dbv' file will be used repeatedly.

HERE'S THE BAD NEWS

If no email addresses could be found, the virus will target newsgroups instead. If the '%windir%\nntpgroups.dat' file exists, the virus will read the newsgroup server name from there. If the file does not exist, the virus attempts to read the newsgroup server from the '%windir%\swen0.dat' file, then deletes the file. If the 'swen0.dat' file did not exist, the virus chooses a random newsgroup server from the '%windir%\swen1.dat' file.

The virus connects to the newsgroup server and requests a list of all valid newsgroups, then writes to the '%windir%\nntpgroups.dat' file the newsgroup server name and the names of any newsgroups that contain more than ten messages.

If the newsgroup server allows posting, the virus randomly posts a single message to all newsgroups in the list from the 'nntpgroups.dat' files. The post will appear to come from the 'VicName' value in the registry, if it exists, otherwise it will be the user's name as returned by the GetUserName() API, the computer name as returned by the GetComputerNameA() API, or the word 'unknown' if neither of the previous APIs returns a valid value. The name

is followed by 6–15 random lower-case letters, which can be optionally followed by '-' or '_', followed by four to eight random lower-case letters. Then comes the '@', followed by between three and five random lower-case letters. The address always ends with '.net' or '.com'. The virus can also choose randomly to make this part of the address blank.

The virus can choose randomly to make the 'NEWSGROUPS' line begin with none or one of 'Microsoft' or 'MS', which can be optionally followed by 'Corporation' or 'Commercial'. This is always followed by 'Client', 'User', 'Consumer', 'Customer', or 'Partner'. The virus can choose randomly to make this line blank.

The 'SUBJECT' line can optionally begin with 'FW:', 'FWD:', or 'RE:', which is always followed by 'Check', 'Take a look at', 'Check out', 'See', 'Prove', 'Watch', 'Taste', 'Use', 'Try', 'Apply', 'Try on', 'Install', or 'Look at'. This may be followed by 'this', 'the', 'these' or 'that', and may be followed by 'correction', 'critical', 'corrective', 'internet', 'security', or 'important'. It is always followed by 'update', 'package', 'patch' or 'pack'.

This can optionally be followed by one of the following options:

1. the word 'for' may be followed by 'MS' or 'Microsoft'. This is always followed by 'Internet Explorer' or 'Windows'.
2. 'that' or 'which', followed by 'comes' or 'came', followed by the word 'from'. This may be followed by the word 'the'. This is always followed by one of: 'M\$', 'Microsoft' or 'MS', and may be followed by 'Corp.' or 'Corporation'.

From this point, the rest of the message is exactly as described previously, beginning with 'this is the latest version of security update'.

For each newsgroup in the list, the virus requests all of the news items that exist. If the 'LISTGROUP' command is not supported (it is not defined in RFC 977), the virus requests every news item in a random range between the years 1980 and 1999. The virus extracts the email addresses from each of the news items and adds these addresses to the '%windir%\germs0.dbv' file, which will be used the next time the email routine runs.

CONCLUSION

We were lucky, in a way – the bugs in W32/Swen may have prevented it from becoming as widespread as it could have been. Now that the *Microsoft* patch email trick has been played, people won't be fooled by that anymore. Or will they? Some people do have short memories ...