Effizienter Viren-Schutz auf E-Mail Gateways

Dr. Erwin Hoffmann

feh@fehcom.de

http://www.fehcom.de

FFG - Frühjahrsfachgespräch

Bochum, 2004-3-11

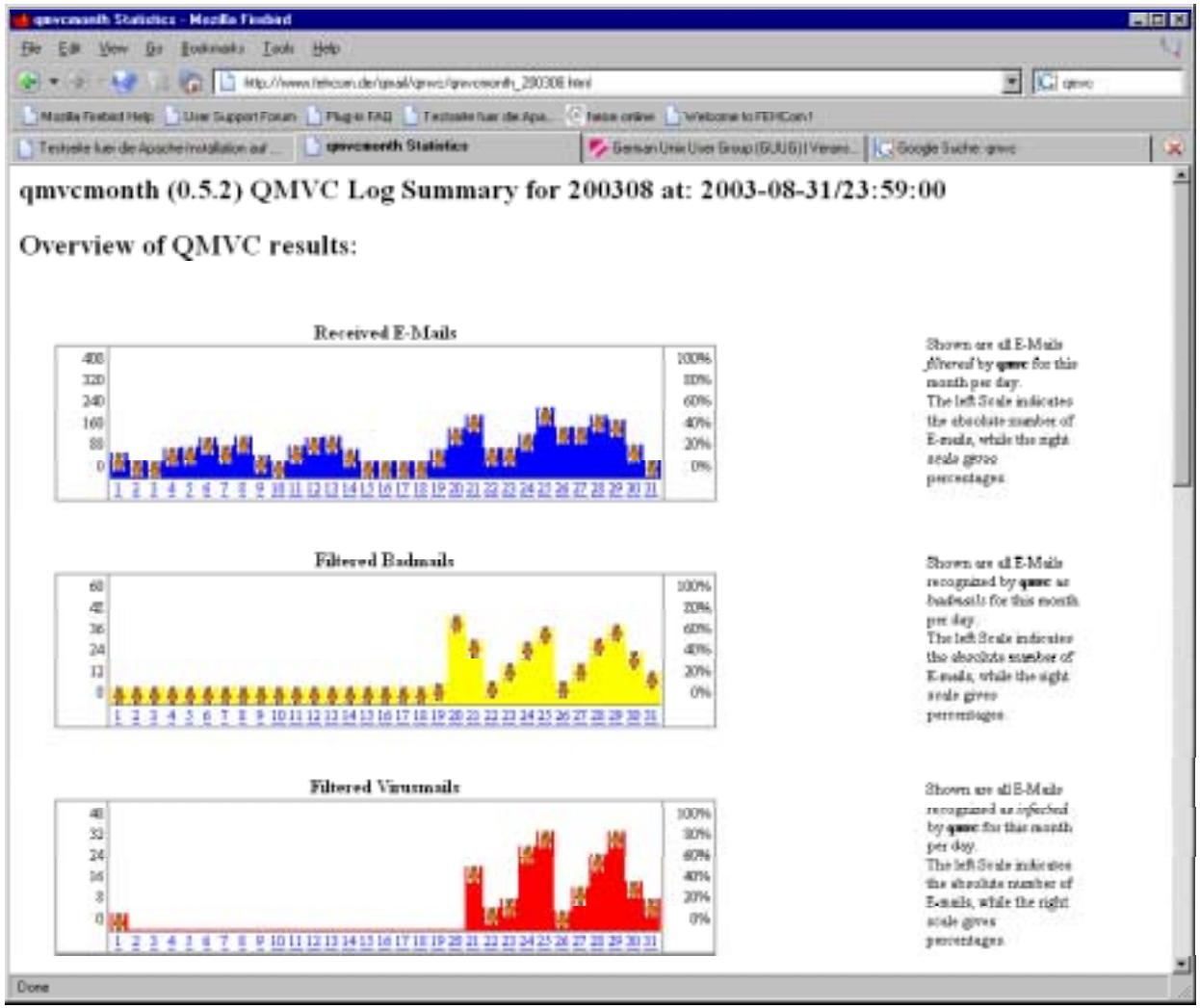
In der Presse

http://www.heise.de/newsticker/meldung/45207:

- Dass mittlerweile schon während eines Tages gleich mehrere neue Schädlingsmutationen auftauchen, macht es den Antiviren-Unternehmen nicht leichter, stets aktuelle Virenpattern zur Verfügung zu stellen.
- Mittlerweile müssten sich die Anwender eigentlich also täglich neue Virenpattern besorgen, um auf dem aktuellen Stand zu bleiben.

  – WDR 2 Nachrichten 5.3.04/15.00 Uhr
  – BSI 5.3.04

Die Sobig-Attacke - August/2003



- QMVC/virulator Auswertung meiner an ***@fehcom.de*** gesendeten E-Mails

Die Auswirkungen

- Heutige Viren-Epedimien stellen DDoS (distributed Denial of Service) Attacken auf E-Mail Gateways dar. Die Viren bringen eine eigene SMTP-Engine mit, über die sie auf den infizierten Rechnern vervielfältigen.
- Zusätzlich zu
  - den normal zu bearbeitenden E-Mails,
  - den zu filterenden Spam-E-Mail
  - müssen nun auch noch die Viren gescannt werden.
- Hierdurch verzögert sich die Zustellung "legitimer" E-Mail teilweise über Stunden.
- Die Administratoren sind busy, die neuen Virenpattern aufzuspielen und infizierte Rechner zu isolieren.

Die Antworten der Industrie

- Hersteller von Anti-Viren Produkten haben Konjunktur; es gibt einige neue Hersteller auf dem Markt (der traditionell von Sophos, NAI und wenigen anderen besetzt ist).
- Es reicht nicht mehr aus, nur einen Virenscanner einzusetzen.
- Virenscanner sind sowohl auf den E-Mail Gateways, den GroupWare-Servern (Exchange, Domino, GroupWise) als auf den Desktop-Systemen angeraten.
- Dies bringt erhebliche Lizenz-, Wartungs- und Administrationskosten mit sich.
- Teilweise sind die Patternupdates wenig effizient (~ 7 MB/Patternfile).
- Einen Schutz gegen neuartige Viren bietet keine dieser Massnahmen.

Die Antwort der OpenSource Gemeinde

Die klassischen AV-Tools für E-Mail-Server wie

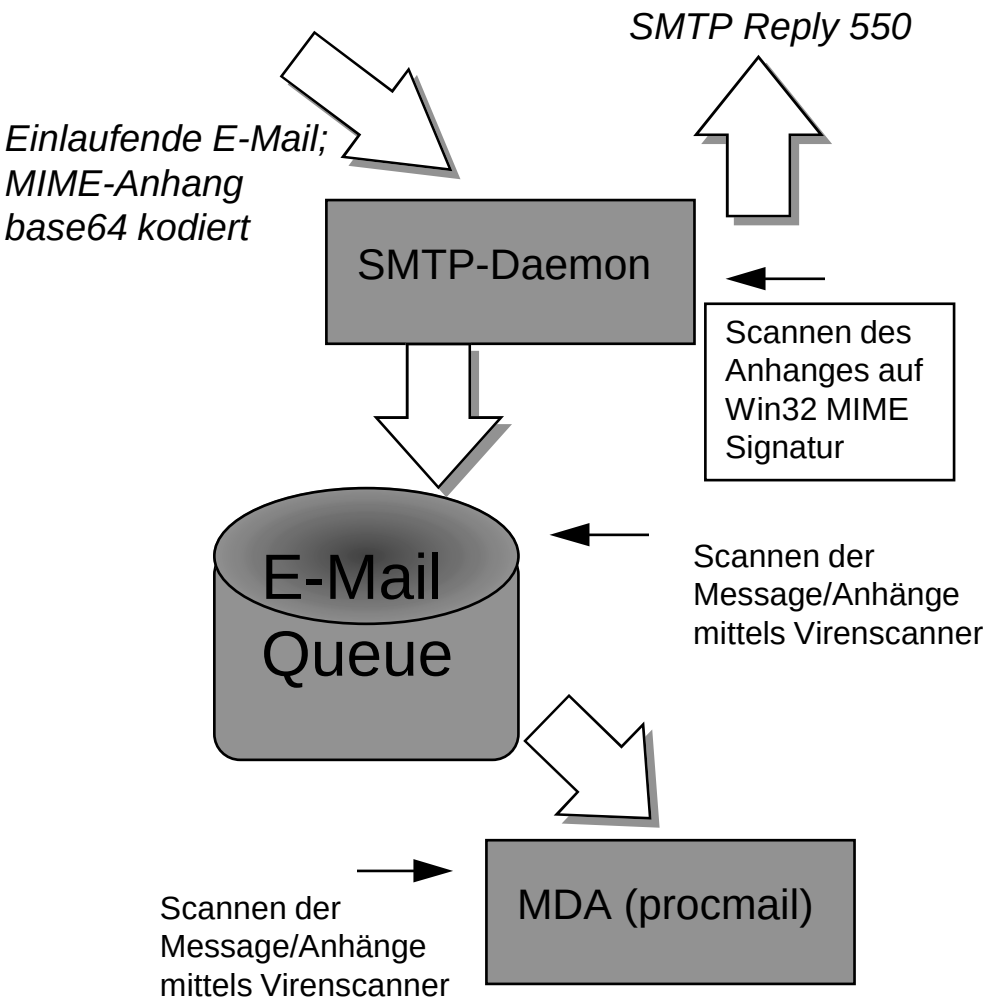
- AMaVis und
- qmail-scanner bzw. scan4virus

versuchen, die eingebundenen AV-Scanner immer effizienter einzusetzen, z.B. durch die SAVI-Schnittstelle bei Sophos (sophie), fsavd bei fsav (Daemon-Mode).

Der Erfolg dieser Massnahmen wird jedoch durch das hohe Spam-Aufkommen konterkariert.

- Statt Viren zu scannen, werden immer häufiger Windows-Executables (in MIME-Anhängen) blockiert.

Der nächste Schritt



Die meisten Windows Executables lassen sich aufgrund der ersten (base64 kodierten) Bytes im erkennen:

- TVqQAAMAA
- TVpQAAIAA
- TVpAALQAc
- TVpyAXkAX
- TVrmAU4AA
- TVrhARwAk
- TVoFAQUAA
- TVoAAAQAA
- TVoIARMAA
- TVouARsAA
- TVrQAT8AA
- # *.zip
- # UEsDBAkAA
- # *.z (gnu-zip)
- # H4sIADWWb
- # double Base 64 Windows Executable
- VFZxUUFBT
- # triple Base 64 Windows Executable
- VkZaeFVVR

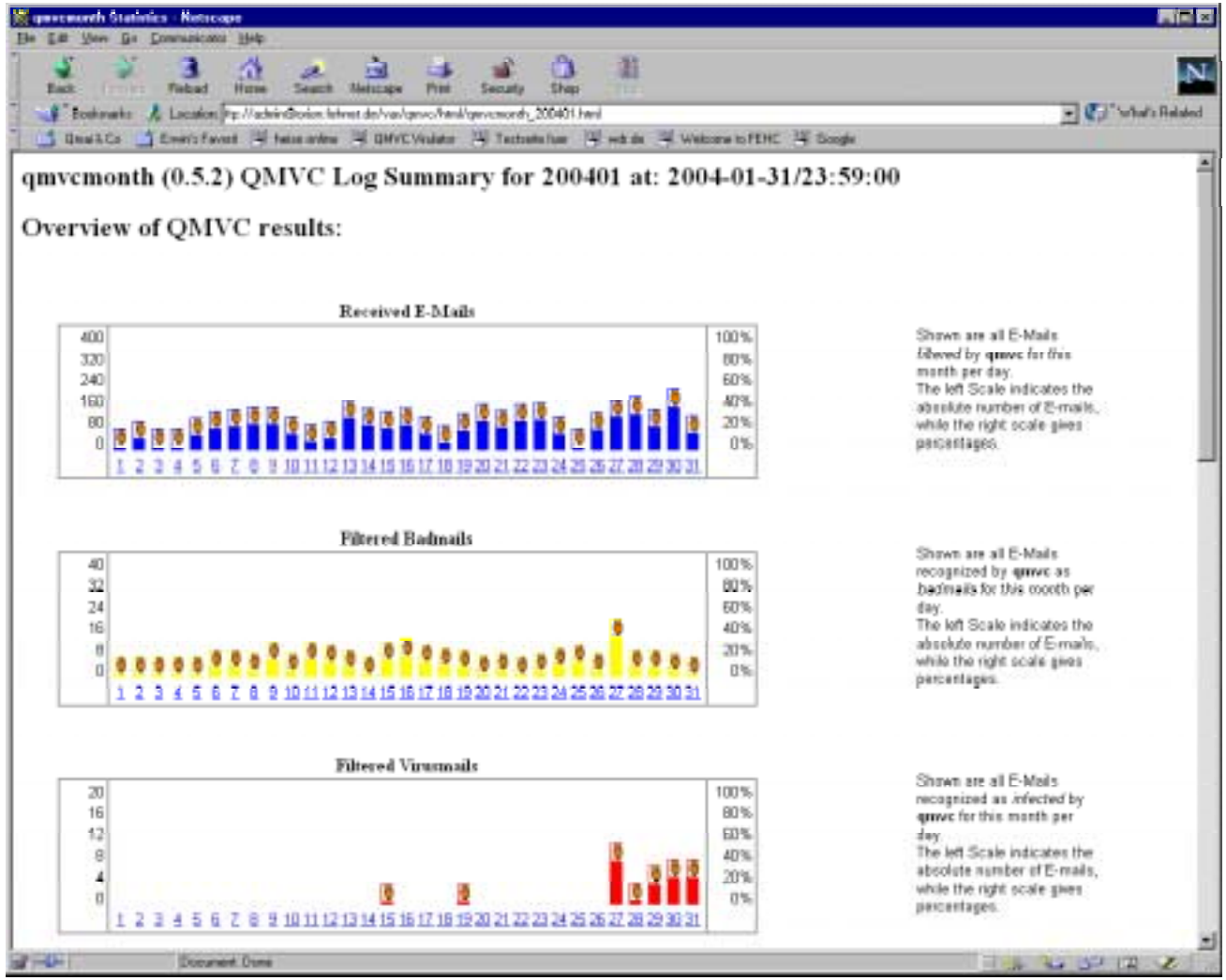
Die ersten Erfolge

Für Qmail gibt es ein "qmail-smtpd-virusscan-1.x.patch", das Windows Executables in MIME-Attachments ausfindig macht und den Empfang der E-Mail per SMTP "550" Return-Code abweist.

Dieses Patch ist Teil meines SPAMCONTROL.

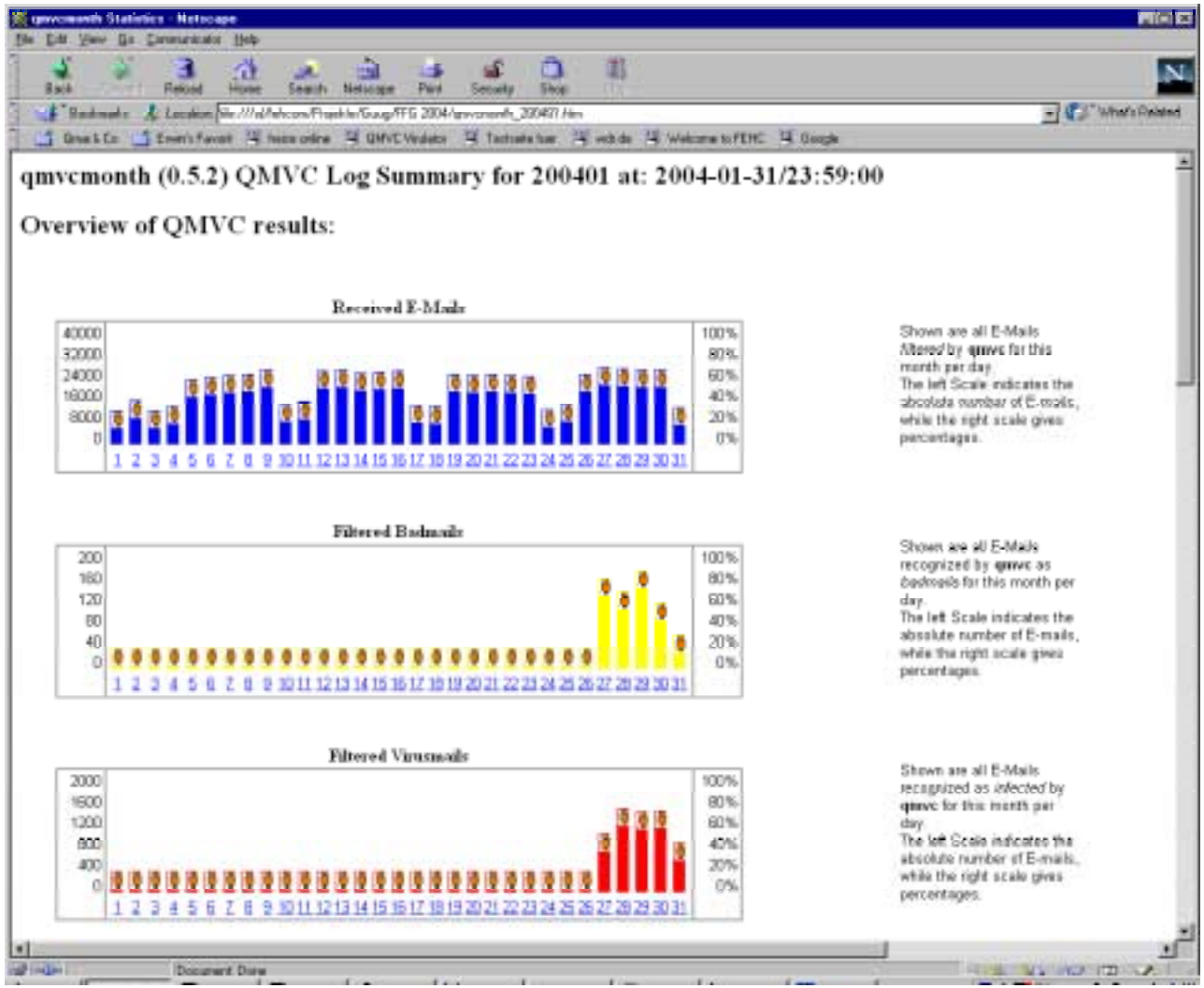
	01/2004	02/2004
Eingelaufene E-Mails	1.281.613	1.415.224
Abgewiesene Spam-Versuche	470.561	555.361
E-Mails mit Windows-Execs	61.712	92.710

Die MyDoom-Attacke - Januar/2004



- QMVC/virulator Auswertung meiner an ***@fehcom.de*** gesendeten E-Mail

... und die MyDoom-Viren kommen durch ...



MyDoom ist ein Transport-Stealth Virus:

- Das Virus tarnt sich als ZIP-Archiv; enthält aber trotzdem einen unter Windows auführbaren Teil.

Es reicht also nicht mehr, auf die MIME-Signatur zu filtern ....

Wir inspizieren das MyDoom-Virus

```
Received: from waldorf-gmbh.de ([194.126.121.218]) by kdmail.netcologne.de
        (Post.Office MTA v3.5.3 release 223 ID# 127-61375U6500L550S0V35)
        with ESMTP id de for <feh@fehcom.de>;
        Thu, 29 Jan 2004 19:16:54 +0100
From: dave@waldorf-gmbh.de
To: feh@fehcom.de
Subject: test
Date: Thu, 29 Jan 2004 20:18:16 +0200
MIME-Version: 1.0
Content-Type: multipart/mixed;
      boundary="----=_NextPart_000_0006_8E972B85.6E7646EC"
X-Priority: 3
X-MSMail-Priority: Normal

This is a multi-part message in MIME format.

------=_NextPart_000_0006_8E972B85.6E7646EC
Content-Type: text/plain;
      charset="Windows-1252"
Content-Transfer-Encoding: 7bit

The message contains Unicode characters and has been sent as a binary attachment.


------=_NextPart_000_0006_8E972B85.6E7646EC
Content-Type: application/octet-stream;
      name="file.zip"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
      filename="file.zip"

UEsDBAoAAAAAAEiSPTDKJx+eAFgAAABYAAAIAAAAZmlsZS5zY3JNWpAAAwAAAAQAAAD//wAAuAAA
AAAAAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABQRQAATAEDAAAAAAAAAAAAAAAA
AOAA
```

Was sagt QMVC ?

attachments:

- 138133103-1075406736.3295-0.orion.fehnet.de: ASCII English text
- 138133103-file.zip: Zip archive data, at least v1.0 to extract

viruslog

- +++ AV Scanner F-Secure : file.zip] : W95/Mydoom.A@mm
- +++ AV Scanner McAfee : FILE.SCR : W32/Mydoom@MM
- +++ AV Scanner CA InoculateIT : file.zip:file.scr : Win32/Shimg.Worm

MyDoom ist ein Transport-Stealth Virus

- Der Anfang der Datei "files.zip":

```
00000000  50 4b 03 04 0a 00 00 00  00 00 48 92 3d 30 ca 27  |PK........H.=0.'|
00000010  1f 9e 00 58 00 00 00 58  00 00 08 00 00 00 66 69  |...X...X......fi|
00000020  6c 65 2e 73 63 72 4d 5a  90 00 03 00 00 00 04 00  |le.scrMZ........|
00000030  00 00 ff ff 00 00 b8 00  00 00 00 00 00 00 40 00  |..............@.|
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

... und das (üble) Ende:

```
000056a0  00 00 00 00 00 00 0c c3  00 00 00 00 00 00 73 00  |..............s.|
000056b0  00 80 00 00 00 00 4b 45  52 4e 45 4c 33 32 2e 44  |......KERNEL32.D|
000056c0  4c 4c 00 41 44 56 41 50  49 33 32 2e 64 6c 6c 00  |LL.ADVAPI32.dll.|
000056d0  4d 53 56 43 52 54 2e 64  6c 6c 00 55 53 45 52 33  |MSVCRT.dll.USER3|
000056e0  32 2e 64 6c 6c 00 57 53  32 5f 33 32 2e 64 6c 6c  |2.dll.WS2_32.dll|
000056f0  00 00 4c 6f 61 64 4c 69  62 72 61 72 79 41 00 00  |..LoadLibraryA..|
00005700  47 65 74 50 72 6f 63 41  64 64 72 65 73 73 00 00  |GetProcAddress..|
00005710  45 78 69 74 50 72 6f 63  65 73 73 00 00 00 52 65  |ExitProcess...Re|
00005720  67 43 6c 6f 73 65 4b 65  79 00 00 00 6d 65 6d 73  |gCloseKey...mems|
00005730  65 74 00 00 77 73 70 72  69 6e 74 66 41 00 00 00  |et..wsprintfA...|
00005740  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00005820  00 00 00 00 00 00 50 4b  01 02 14 00 0a 00 00 00  |......PK........|
00005830  00 00 48 92 3d 30 ca 27  1f 9e 00 58 00 00 00 58  |..H.=0.'...X...X|
00005840  00 00 08 00 00 00 00 00  00 00 00 00 20 00 00 00  |............ ...|
00005850  00 00 00 00 66 69 6c 65  2e 73 63 72 50 4b 05 06  |....file.scrPK..|
00005860  00 00 00 00 01 00 01 00  36 00 00 00 26 58 00 00  |........6...&X..|
```

Transport-Stealth Viren lassen sich aufgrund ihrer Loader-Anweisungen für das Windows Betriebssystem erkennen:

- KERNEL32.DLL
- W32_32.DLL
- ....

Loader-Type Identifizierung

- In Ergänzung zur MIME-Type Identifizierung von ausführbaren Dateien, kann auch eine Loader-Type Erkennung vorgenommen werden.
- Dies wird Teil des Releases 1.7 von QMVC werden.
- Den generischen Teil der Loader-Type Identifizierung werde ich nach C portieren und innerhalb von SPAMCONTROL für Qmail verfügbar machen.
- Es ist zu erwarten, dass diese Methode auch für andere E-Mail Programme eingesetzt werden kann.
- Es bleibt die Hoffnung, damit effektiv und effizient ein Anti-Virus Schild aufstellen zu können, das zudem auf MacOS/LINUX übertragbar ist und sich nicht ohne weiteres umgehen lässt.

Die nächste Attacke (W32/Netsky.c@MM)

```
From: cymes@poczta.fm
To: feh@fehcom.de
Subject: something is not ok
Date: Fri, 5 Mar 2004 20:29:24 +0100
MIME-Version: 1.0
Content-Type: multipart/mixed;
      boundary="----=_NextPart_000_0011_00003DE9.000009CE"
X-Priority: 3
X-MSMail-Priority: Normal
Message-Id: <20040305192522.2E4211A0054@mrbusi1.netcologne.de>
#### Error reports (internal, file, find) ....
#### Attachment results ....
2933127971-1078517199.28601-0.orion.fehnet.de: ASCII text
2933127971-ranking.zip:                    Zip archive data, at least v1.0 to extract
+++ Found 2 attachments;  thereof 2 positive for scanning
#### Badmail reports ....
#### Bad Loader Type ( 2 criteria met):
+++ KERNEL32.dll + ADVAPI32.dll |<=>| Win32 (ranking.zip @lines 20 + 24)
+++ KERNEL32.dll + WS2_32.dll |<=>| Win32 (ranking.zip @lines 20 + 22)
#### Virus reports ....
#### AV scanner uvscan found 1 virii:
+++ W32/Netsky.c@MM |<=>| ranking.zip/RANKING.HTM.SCR
#### Actions on incident ....
+++ The blocked E-Mail (BadLoaderType) is kept in /var/qmvc/kept as " cymes@poczta.fm.2933127971"
+++ The blocked E-Mail (VirusInfected) is kept in /var/qmvc/kept as " cymes@poczta.fm.2933127971"
#### Reactions on incident ....
+++ Notify_Receiver_if_BadLoaderType:  feh@fehcom.de
```