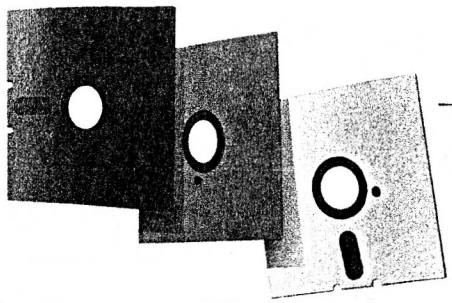

Trojanische Programme

Trojanische Pferde sind uns ja aus der Geschichte bekannt. Was aber hat es mit den trojanischen Programmen auf sich, die auch alte Computer-Hasen in Panik versetzen?

Die trojanischen Pferde waren einmal eine ganz brauchbare Methode, um Soldaten unbemerkt in eine feindliche Stadt einzuschleusen. Daß wir uns wieder mit der griechischen Geschichte beschäftigen müssen, hat seinen Grund in dem merkwürdigen Humor einiger Computerfans. In den USA tauchen in letzter Zeit in den Mailboxen (Bulletin Boards) sogenannte trojanische Programme (in MS-DOS) auf.

So ein Programm sieht genauso aus wie das Original, lediglich die Versionsnummer ist manchmal geändert, man freut sich also auf eine neue Version. Aber irgendein seltsamer Zeitgenosse hat das Programm etwas verändert. Wenn man so ein Programm dann laufen läßt, sind die Folgen fürchterlich: Die Disketten werden neu formatiert, die Festplatte gelöscht und derlei schlimme Dinge mehr.

Wie man sich dagegen schützen kann? Fast unmöglich. In Deutschland ist die Situation etwas besser, da hier viel Public-Domain-Software über Firmen vertrieben und nicht direkt aus Mailboxen geholt wird. Die Versorgung mit Public-Domain-Software in den USA wird dagegen fast ausschließlich über große Mailboxen abgewickelt.

Unsere amerikanische Schwesterzeitschrift Dr. Dobb's Journal berichtet in Ausgabe 2/86 über diese trojanischen MS-DOS-Programme, die über kurz oder lang sicherlich auch in Deutschland auftauchen werden. Wir wollen Ihnen diese Liste nicht vorenthalten:

ARC513.EXE

Dieses Programm wirkt wie eine neue Version des Archivierungsprogramms ARC. ARC513 beschreibt jedoch die Spur null der Diskette oder der Harddisk und zerstört sie dadurch. Version ARC512 ist in Ordnung.

BALKTALK

Auch dieses Programm schreibt auf den Datenträger und zerstört ihn dadurch. Die Unterscheidung zwischen guter und gefährlicher Version ist schwierig, rechnen Sie deshalb immer mit dem Schlimmsten!

DISKSCAN.EXE

Programme aus dem amerikanischen PC-Magazin, um auf einer Festplatte nach defekten Sektoren zu suchen. Die Troja-Version erzeugt hingegen defekte Sektoren...

SCANDAD.EXE
(wie DISKSCAN.EXE)

BADDISK.EXE
(wie DISKSCAN.EXE)

DOSKNOWS.EXE

Ein System-Status-Utility. Steht im Verdacht, auch ein trojanisches Programm zu sein. Das ungefährliche Original ist 5376 Byte lang.

EGABTR

In der Beschreibung ist zu lesen, daß das Programm den EGA-(Enhanced Graphics Adapter-)Display verbessert. Aber es löscht alles, was zu löschen ist und schreibt »Arf! Arf! Got you!« auf den Bildschirm.

FILER.EXE

Wird in der Beschreibung als großartiges neues File-System bezeichnet, löscht aber »nur« die Festplatte.

SECRET.BAS

In der Beschreibung steht, daß dieses Programm nicht richtig läuft. Jemand möge es bitte testen. Wenn es gestartet wird, formatiert es alle Disketten, die der Benutzer einlegt.

VDIR.COM

Produziert einen Systemabsturz und formatiert alles was erreichbar ist.

DROGAN.COM

Dieses Programm ist eine »überarbeitete« Version des PC-DOS FORMAT.COM. Es ist 7040 Byte lang und schreibt nach dem Start »Please wait...« auf den Bildschirm. Sodann laufen die Laufwerke an und es erscheint die Meldung »BYE F__HEAD«, und die Disketten sind neu formatiert.

QUIKRBBS.COM

Dieses Programm lädt angeblich die Botschaften-Datei der Mailbox doppelt so schnell wie normal. In Wirklichkeit kopiert es die Mailbox-Kontrolldatei RBBS-PC.DEF (enthält unter anderem alle Paßwörter der Mailbox-User!) in eine ASCII-Datei namens HISCORES.DAT. Damit wäre die Mailbox geknackt.

STRIPES.EXE

Zeichnet eine hübsche amerikanische Fahne auf den Bildschirm und kopiert währenddessen die Datei RBBS-PC.DEF auf die Datei STRIPES.BQS (Effekt: siehe QUIKRBBS.COM).

Die beiden letzten Programme sind insbesondere für Sysops wichtig, die alle Uploads prüfen. Dazu muß man noch wissen, daß nahezu alle amerikanischen Mailboxen das gleiche Mailboxprogramm auf einem IBM-PC/XT/AT oder kompatiblen Computer benutzen.

Zu Hilfe!

Wie kann man sich nun vor solchen Programmen schützen? Es ist zunächst immer Vorsicht geboten, wenn dem Programm kein Quelltext beigefügt ist. Den Test unbekannter Programme sollte man lieber auf einem Computer ohne Festplatte machen. Vorsicht bei obskuren Mailboxen. Der Sysop einer guten Mailbox testet ein Programm, bevor er es für ein Download frei gibt. Dabei muß er natürlich auf Programme wie QUIKRBBS und STRIPES achten, damit seine Mailbox nicht geknackt wird.

Uns ist das Programm CHK4BOMB (sprich »check for bomb«) aufgefallen, das Programme auf »trojanische Fähigkeiten« prüft. Das Programm listet alle ASCII-Zeichenfolgen des zu testenden Programms auf dem Bildschirm. Damit fallen eventuelle hämische Bemerkungen auf (siehe EGABTR und DROGAN). Außerdem prüft es auf Routinen, die auf Diskette oder Harddisk zugreifen. Die folgenden Warnungen gibt das Programm bei der Prüfung aus:

```
****WARNING**** This
program writes to absolute
sectors.
```

Dieses Programm schreibt absolute Sektoren. Dadurch besteht die Gefahr, daß Daten überschrieben werden.

```
****WARNING**** This pro-
gram FORMATS a disk!
```

Dieses Programm formatiert eine Diskette oder die Harddisk. Wenn das geschieht, sind alle Daten auf der Diskette oder der Harddisk unwiderruflich weg.

```
****WARNING**** This pro-
gram uses the ROM BIOS
routines for direct disk
access!
```

Dieses Programm benutzt die BIOS-Routinen im ROM für direkten Zugriff auf Diskette oder Harddisk.

Wer eine dieser Warnungen vom Programm CHK4BOMB erhält, sollte bei der Benutzung des getesteten Programms mit dem Schlimmsten rechnen und entsprechend vorsichtig sein.

Wir bitten jeden Leser, der einem solchen trojanischen Programm aufgesessen ist oder von der Existenz weiterer Programme dieser Art weiß, uns die Namen dieser Programme mitzuteilen, damit wir die anderen Leser warnen können.

(Rainer W. Gerling/ts)

Info: CHecK 4 BOMB, Version 1.00 vom 29.10.1985, geschrieben von Andy Hopkins. Kontakt: Bob Klahn's BBS (Fido 107/50, 001-302-764-7522, 2400/1200 Baud) in Wilmington, Delaware, USA.