Harte Nüsse für die Opfer

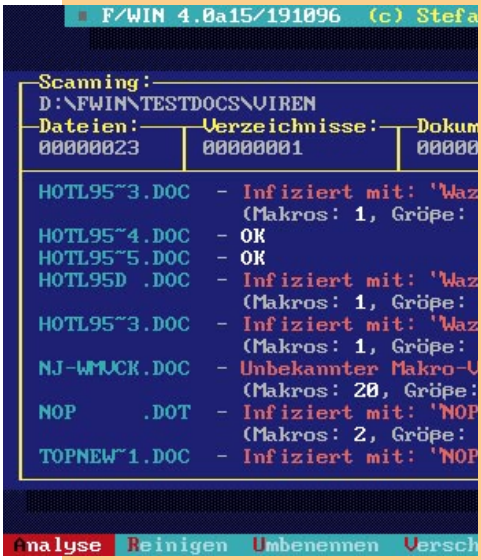
Recht produktiv ist ein „Lord Nutcracker“, obwohl er ständig das Ende seiner Fleißarbeit ankündigt. Schon mehrere Dutzend *Nutcracker*-Viren sind mittlerweile bekannt, die teilweise neue Infektionsstrategien verwirklichen und eine Desinfektion sehr erschweren. So verändern die Viren zwar Einträge im Master Boot Sector, jedoch anders als die üblichen Schädlinge, die beim Rechnerstart aktiv werden. Der oft hilfreiche Befehl FDISK /MBR versagt daher – nur Antivirenprogramme oder Spezialisten helfen weiter.

Gefährlich sind die Viren in doppelter Hinsicht: Wenn ein springender Ball (ähnlich wie beim Ping-Pong-Virus) erscheint, bestrafen sie den Versuch eines Warmstarts: Beim Drücken der [Strg][Alt][Entf]-Tasten löschen die Viren unter Umständen einzelne Sektoren der Festplatte. Das gleiche passiert, wenn sie sich beobachtet fühlen, genauer: wenn jemand Virencode auf die Diskette kopiert.

ANTIVIRENPROGRAMM

F/Win 4.0: Noch immer nur unter DOS, aber ein probates Mittel gegen die Flut der Makroviren

Zwei Waffen setzt das neue F/Win ein, um (die vielen) Makro- und (die wenigen) Windows-Viren zu erkennen: Die schon bekannten Exemplare identifiziert es eindeutig, indem es ihre Programmsequenz mit einer gespeicherten Prüfsumme vergleicht. Völlig neue Viren können mit hoher Wahrscheinlichkeit erkannt werden, da die Infektionsstrategien für diese Virentypen relativ überschaubar sind.



...kurz notiert

■ Kaum jemand wußte, daß **Dr. Solomon's Anti-Virus Toolkit** von S&S International stammt. Jetzt nennt sich der Hersteller nach seinem Hauptprodukt „Dr. Solomon's Software“ (Luisenweg 40, 20537 Hamburg, Tel. (040) 25 19 54-0, Fax 251954-50).

■ Nicht nur Antivirenservice, sondern auch Hilfe bei anderen PC-Problemen bietet **PC-TuneUp** (http://www.tuneup.com) Windows-95-Nutzern per Internet gegen eine Monatsgebühr von rund 4 Dollar. Einen Monat lang darf kostenlos geschnuppert werden.

■ Nach Viren in der E-Mail sucht **Mimesweeper** (Integralis, 81671 München, Tel. (089) 450 660-0, Fax 450 660-33). Die Version 2.4 soll deutlich schneller sein und mit Windows NT 4.0 zusammenarbeiten.

Virus statt Hilfe von Microsoft

Tagelang hat Microsoft im Internet eine virenverseuchte Datei angeboten, selbst als die zuständige Geschäftsstelle bereits informiert war.

Wer Mitte Oktober auf den Schweizer Web-Seiten von Microsoft Hilfe suchte und an die Datei HOTL95D.DOC geriet, hatte ein neues Problem: Außer Hotline-Nummern enthielt sie den *Wazzu*-Virus (siehe rechts). Zuvor hatte das Unternehmen die virenverseuchte Datei per CD („Letz Fetz on the Inter-Netz“) auch schon auf der Orbit-Computermesse in Basel verschenkt. Fazit: Sogar der Winword-Hersteller bekommt die auf seine Software spezialisierten Viren nicht in den Griff.

Wazzu aktiv

Unter den über 100 bekannten Makroviren (Stand: Ende Oktober) tut sich der Oldtimer *Wazzu* besonders hervor. Im Unterschied zu anderen häufigen Winword-Viren wie NOP ist er nicht für die deutsche Textverarbeitung programmiert. Da er keine sprachabhängigen Befehle verwendet, läuft er aber auch hier. Seine Schadfunktion: In befallenen Dokumenten kann an unvorhersehbaren Stellen „wazzu“ stehen, der Spitzname der Washington State University (siehe CHIP 9/96, Seite 14).