



VIREN

Deutsches Winword im Visier der Rachegöttin



Jetzt wird es auch im deutschen Sprachraum ernst: „Evil One“ lautete der Absender einer Nachricht, mit

der Ende Februar ein Winword-Virus im Internet verbreitet wurde. Sein Ziel ist deutschsprachiges Winword ab der Version 2.0c. Bisher stammten Word-Makroviren meist aus dem Ausland. Das deutsche Textverarbeitungsprogramm ist gegen sie recht immun, auch wenn Formatvorlagen Schaden nehmen.

Nemesis ist rund 25 Kilobyte groß und versucht vergeblich, einen Neuroquila-Virus abzusetzen. Autor soll ein 16jähriger einschlägig bekannter Schüler aus Wien sein. Der nach einer griechischen Göttin benannte Virus ersetzt beim Drucken einer Datei die letzte Zeile durch einen Hinweis auf eine „Nemesis Corporation“.

Abschied

Alan Solomon zieht sich aus der ihm und seiner Frau gehörenden Antiviren-Firma S&S International zurück. *Dr. Solomon's Anti-Virus Toolkit* wird seinen Namen behalten. Der promovierte Mathematiker will im Datenrettungsgeschäft aktiv bleiben und denkt auch über neue Antiviren-Projekte nach.

Das Ehepaar soll als Kaufpreis über 20 Millionen Pfund bekommen haben. *Brain*, den Urahn der PC-Viren, hatte Solomon als einer der ersten analysiert. Die Unternehmersgattin kurbelte noch als Teilzeitmutter den Vertrieb des Gegenmittels an.

... in aller Kürze

Eine Einführung in die Computersicherheit stellt die amerikanische Behörde NIST online zur Verfügung (<http://csrc.nist.gov/nistpubs/800-12>).

Das Verschlüsselungswerkzeug **Blockit** und das mit Verschlüsselung arbeitende Zugriffskontrollsystem **Tenc** bietet Norman Data Defense Systems, Broßhauser Str. 28, 42697 Solingen, Tel. (0212) 26718-0, Fax 26718-15.

Alle **Escom-Rechner** sind seit Februar mit einer Thunderbyte-Testversion ausgestattet.

Russischer Zeitzünder in Dokumenten

Hot heißt der derzeit wohl gefährlichste internationale Winword-Virus. Zur Verbreitung verhalf ihm – erstmals bei Makroviren – eine Zeitbombe. Der über Word-Dokumente in Rußland verbreitete Übeltäter verhält sich

zunächst unauffällig, notiert allerdings ein Auslösedatum. Erst zwei Wochen nach der Infektion schreitet er zur destruktiven Tat. Dann löscht er unter Umständen das Dokument, das man gerade öffnen und bearbeiten möchte.

DOS-Jäger pirscht sich an Windows-Viren an

Einen Schönheitsfehler hat es für Windows-Gewohnte allemal: *F/Win* sucht auf Windows spezialisierte Viren, ist selbst aber DOS-Software.

Das Programm geht nach Faustregeln vor, erkennt also möglicherweise auch Schadprogramme, die erst in den nächsten Monaten oder Jahren auftreten. Die Diagnose der verdächtigen Befehle in Programmen oder Makros erscheint in gut verständlichen Aussagen am Bildschirm.

Den Reim darauf muß sich, trotz einer zusammenfassenden Bewertung, der Anwender selbst machen. Dabei ist Skepsis angebracht: Die sensible Shareware schießt eher über das Ziel hinaus.

Vollversion für ca. 35 Mark bei Stefan Kurtzhals, Dörrenbergstr. 42, 42899 Remscheid, Tel. (02191) 55126

Geballte Virentechnik

So ziemlich alle Register zieht ein Virus, der seit kurzem in Slowenien sein Unwesen treibt: Er ist dank Tarnkappentechnik nahezu unsichtbar, befällt sowohl Bootsektoren als auch Programmdateien und ändert sein Aussehen bei jeder Vermehrung radikal. Außerdem gehört er zu den schnellen Infektoren, der jede Infektionsgelegenheit wahrnimmt, die sich ihm bietet. Sein Name *In_the_Wind* und das Kürzel *Fitw* verweisen auf den Text „Fart in the wind“, den er mit sich herumträgt.

Die vielen Kniffe blähen den Virencode auf; infizierte Dateien sind daher um fast 8 Kilobyte länger. Bei der Disketteninfektion schafft sich der Virus ein geräumiges Versteck. Er greift auf eine normalerweise ungenutzte Spur zu, was die an ihre Grenze getriebenen Laufwerke mit gequältem Rattern quittieren.

Die destruktive Seite kehrt der windige Virus an Montagen nach außen, die ein ungerades einstelliges Datum tragen. Das nächste Mal überschreibt er also wieder am ersten April alle Platten auf infizierten Rechnern mit Datenmüll.

