Zhengxi, der intelligente Wolpertinger

Als wolle der unbekannte Autor sein Gesellenstück abliefern, hat er in *Zhengxi* ziemlich alles eingebaut, was in Viren heute so „in“ ist. Die Software infiziert nicht nur Programmdateien mit den Endungen EXE und OBJ, sondern injiziert auch in komprimierte ZIP-, ARJ- und RAR-Archive ihren ansteckenden Code. Seine Entdeckung und Identifizierung erschwert der Virus, indem er sich bei jeder Reproduktion ein anderes Aussehen gibt (Polymorphie).

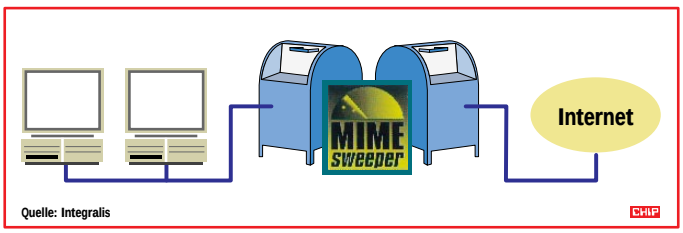
Nicht allein seine stattliche Länge von rund 7 Kilobyte macht den Analysten zu schaffen. Der Virenautor hat kaum einen Trick ausgelassen, um die Einsicht in sein Programm zu erschweren. Sprungziele sind selten als feste Adresse angegeben, sondern werden jeweils errechnet. Statt mit den sonst üblichen Zeichenvergleichen fischt Zhengxi mit Hilfe von Prüfsummen nach Infektionsopfern.

Der extrem destruktive Virus hat es auf alle Dateien und Verzeichnisse ab dem Laufwerk C: abgesehen. Glücklicherweise scheint er – außer in den Sammlungen der Experten – noch nirgendwo aufgetaucht zu sein.

Dies ist um so erfreulicher, als Zhengxi nur schwer aus Dateien zu entfernen ist: Er klinkt sich nicht wie die meisten seiner Kollegen vorne in die Ablaufsequenz eines Programms ein, sondern vertraut darauf, im Befehlsgestrüpp einen Unterprogrammaufruf zu finden. Dort beißt er sich fest und muß daher an einer für die Antiviren-Software zunächst unbekannten Stelle aufgespürt werden.

Hüter der halben Mailboxen

Nach Briefbomben in der elektronischen Post fahndet *Mime Sweeper* auf Windows-NT-Servern. Sowohl vom Lokalen Netz (LAN) als auch von außen ist der Mailbox nichts anzumerken, doch im Inneren dröselt die Software alle Sendungen vorübergehend auf, um unerwünschte Beigaben herauszufischen.



Entwarnung: Mime Sweeper schaltet Briefbomben aus

Der Wächter versteht sich in seiner ersten Version bereits auf elektronische Post à la cc:Mail, Microsoft Mail, MHS und SMTP mit den immer populäreren Beigaben im MIME-Format (Multipurpose Internet Mail Extensions). ZIP-Dateien packt er aus, um an die Bestandteile heranzukommen. LHA-Kompression und UUE-Kodierung sollen in künftigen Versionen berücksichtigt werden.

Zur Diagnose arbeitet das Analyseinstrument mit einem oder mehreren der üblichen Virenscanner zusammen.

Anbieter: Integralis, Trausnitzstr. 8, 81671 München, Tel. (089) 45 6 60-0, Fax 45 06 60-33

Wiedergutmachung

Die englische Microsoft UK unterstützt Schulungsfirmen bei Antiviren-Workshops. Der Sicherheitsspezialist Sophos erhielt personelle Unterstützung und Word-Lizenzen für seinen Kurs mit dem inhaltlichen Schwerpunkt Makroviren. Die Winword-Parasiten sind mittlerweile in den englischsprachigen Ländern zur weitestverbreiteten Virenart aufgestiegen.

In Deutschland sieht der traditionsreichste Veranstalter ähnlicher Kurse kein solches Entgegenkommen des Quasi-Monopolisten. „Das Antivirenprogramm von Microsoft erkennt nach unseren Tests nur rund ein Drittel der existierenden Viren“, ärgert sich Franz-Josef Lang, „und wir dürfen uns mit den Sicherheitslücken herumplagen.“

Anbieter: BFK edv-consulting, Durlacher Allee 47, 76131 Karlsruhe, Tel. (0721) 962 01-1, Fax 962 01-99
EDV-Sicherheitsberatung F.-J. Lang, Wotanstr. 109, 80639 München, Tel. (089) 178 46 16, Fax 178 39 69

Nexiv_Der – wählerischer Späher im PC

Kopfschmerzen dürfte *Nexiv_Der* den Herstellern von Antiviren-Software bereiten, weil er Dateien auf ungewöhnliche Art infiziert. Der Virus beobachtet nämlich die Beuteprogramme bei der Arbeit und schlägt willkürlich zu. Falls die zufällig erwischte Stelle im Programm es dank eines Sprungbefehls oder ähnlicher Sollbruchstellen zuläßt, heftet er sich an das Opfer.

Zur Eigentümlichkeit dieser Jagdmethode gehört, daß der Virus in Opferdateien nur aktiv werden kann, wenn sie mit ähnlichen Parametern oder unter ähnlichen Umständen gestartet werden. Was wie eine miserable Überlebensstrategie klingt, macht es im Verbund mit einer polymorphen Tarnung heutiger Antiviren-Software in vielen Fällen schwer, zwischen Freund und Feind zu unterscheiden. Denn nur unter bestimmten Umständen benimmt sich der willkürlich eingestreute Virencode auffällig.

IN ALLER KÜRZE...

Die **Jahreskonferenz der Eicar** (European Institute for Computer Anti-Virus Research), Hochstallerweg 28, D-86316 Friedberg, Tel. (089) 636-424 42, Fax 636-528 88, findet vom 17. bis 19. November in Hagenberg (Oberösterreich) statt.

Sicherheitssoftware aus Spanien: Antivirus-, Sicherheits- und Verschlüsselungssoftware bietet Panda Software International, Pio Baroja 7, E-28009 Madrid, Tel. (0034 1) 504 29 15, Fax 574 12 08, einzeln unter den Namen Artemis, Buho, Pfence oder kombiniert als Security Toolkit.