Angreifer im PC

Ihr PC wird als Spam-Schleuder missbraucht. Die Passwörter sind ausspioniert, die Kundenkartei geklaut. Wie Sie sich davor schützen, sagt Ihnen PC Professionell in diesem Test.

Wolfgang Nefzger, Burkhard Müller

Zunehmend kapern kriminelle Elemente fremde PCs über das Internet. Die Angreifer wollen nicht ihr Ego aufpolieren oder Freunden imponieren, sie wollen ans große Geld. Gestohlene Passwörter und Kreditkartendaten lassen sich versilbern. Noch einfacher ist es, die ferngesteuerten Rechner zu vermieten – für den Spamversand. Oder wie wär's mit der Erpressung eines Online-Unternehmens? Die international organisierte Mafia ist erfinderisch.

Klingt nach einem schlechten Film, ist aber Realität. Hunderttausende PCs weltweit sind offen wie Scheunentore, sobald sich die Besitzer im Internet bewegen. Treffen kann es jeden: Nach einer Studie von Websense *(www.websense.com/Web@Work/2004)* ist zum Beispiel jeder dritte Firmenrechner mit Spionageprogrammen verseucht.

Der Oberbegriff für Angreifer, die derartige Attacken erlauben: Trojaner oder auch Backdoor (engl. Hintertür). Hinter diesen Bezeichnungen verbirgt sich eine Vielfalt an Schädlingen.

Zombies bilden Botnets

Der Trend bei kriminellen Angriffen geht seit einigen Monaten in eine neue Richtung: Angreifer suchen nicht nur einen einzigen PC, sondern infizieren viele tausend PCs mittels gefährlicher Würmer und Viren. Jeder dieser PCs lässt sich dann über eine Backdoor fernsteuern, er ist bild-

lich gesprochen zum Zombie geworden – ein Jargon-Ausdruck für kompromittierte Rechner. Die Programme, die PCs infizieren, werden Bots genannt. Eine Vielzahl an Bots, die von einem Computer aus ferngesteuert werden, bilden ein Botnet.

Solche Botnets lassen sich für viele Zwecke missbrauchen. Experten gehen zum Beispiel davon aus, dass rund 30 Prozent der weltweit versandten Spam-Mails über Botnets verteilt werden. Weil die Spam-Nachrichten damit viele verschiedene Absender-IP-Adressen haben, sind sie nur schwer abzuwehren. Da mit dem Versand von Spam tatsächlich Geld verdient wird, lohnt sich das finanziell auch für die Betreiber von Botnets.

In jüngster Vergangenheit gab es zudem etliche Erpressungsversuche gegenüber professionellen Websites, etwa Anbietern von Sportwetten. Zahlen deren Betreiber das geforderte Geld nicht, so starten die Erpresser eine Distributed-Denial-of-Service-Attacke (DDoS). Dabei erteilen sie den Zombies im Botnet den Befehl, den Webserver des Opfers mit Datenpaketen zu bombardieren. Dieser kann die Vielzahl von Anfragen nicht bewältigen, so dass er nicht mehr erreichbar ist. Neben dem Image-Schaden verliert ein Online-Shop oder ein Online-Wettbüro damit auch realen Umsatz.

Automatische Infektion

Wie kommen die Trojaner auf die Festplatte? Der klassische Weg führt über Downloads aus dem Internet. Trojaner hängen sich Huckepack an unverdächtige Programme und installieren sich beim Programmstart unbemerkt im Hintergrund. Tauschbörsen wie Kazaa sind dabei eine wahre Brutstätte für Trojaner und Backdoors.

Daneben nutzen moderne Trojaner die üblichen Verbreitungstechniken von Viren und Würmern: Massen-E-Mails, freigegebene Windows-Laufwerke in LAN und Internet sowie Weitergabe mit raubkopierten Programmen. Manche Trojaner nutzen auch gezielt Backdoors, die andere Viren und Würmer auf einem infizierten PC geöffnet haben. Mydoom und Sasser verbreiten sich selbsttätig über Windows-Sicherheitslücken. Sie öffnen Backdoors, über die ein Angreifer seinen Trojaner einschleusen kann. Manche Trojaner suchen selbstständig nach solchen infizierbaren Systemen.

Pflicht: kombinierte Schutzprogramme

Wie für Viren gibt es auch für Trojaner spezielle Scanner, welche die Schädlinge aufspüren und entfernen sollen. Für diesen Vergleichstest infizieren die *PC-Professionell*-Tester ein Windows-XP-System mit 433 verbreiteten Trojanern und testen unter anderem die Erkennungs- sowie die Entfernungsrate. Zum Vergleich wird Norton Antivirus 2004 als bekannter Vertreter der Virenscanner-Fraktion herangezogen. Arbeiten Trojanerscanner tatsächlich besser als Virenscanner?

»Trojanerscanner schützen unzureichend. Nur ein Paket aus Virenscanner, Desktop-Firewall und Antispam-Tool bietet perfekten Schutz.«

Software-Redakteur **Burkhard Müller**

Das Ergebnis sieht für die Trojanerscanner nicht gut aus: Der Testsieger Trojan Defence Suite verfügt über die beste Erkennungsrate von 93 Prozent, ist also etwas besser als Norton Antivirus mit 90 Prozent. Digital Patrol und Ewido folgen mit je 82 Prozent. Bei der Entfernungsrate sieht es noch schlechter aus: Das Norton-Produkt entfernt immerhin 78 Prozent, gefolgt von Digital Patrol mit nur 63 Prozent und Ewido mit 60 Prozent. Sieben der elf Kandidaten können nicht einmal die Hälfte aller Schädlinge entfernen.

Nur die Erkennung der 433 Test-Trojaner als Datei auf der Festplatte beherrscht Trojan Defence Suite als einziger Scanner etwas besser als Norton Antivirus. Beim Reinigen der Registry sind einige Scanner zwar erfolgreicher als Norton, doch löscht Norton dafür alle Trojanerdateien, die Registry-Einträge sind damit wirkungslos. Für unerfahrene Anwender ist ein gutes Antivirenprogramm deshalb die bessere Wahl. Zusätzlich gehört eine Desktop-Firewall auf jeden PC. Wer dagegen Trojanern und anderen schädlichen Programmen auf Prozessebene selbst nachspüren will (siehe »Know-how: Spione enttarnen«, Seite 126), greift zu Trojan Defence Suite. BMU

Empfehlung der Redaktion

Keine Empfehlung der Redaktion

Sämtliche Trojanerscanner im Test können nicht überzeugen. Sie scheitern allesamt daran, einen infizierten PC vollständig zu säubern. Deswegen gibt es keine Empfehlung.

	Produkt Hersteller	(maximal 100 Punkte)
1	**Trojan Defence Suite 3** Diamond CS	76,8
2	**Spionage-Abwehr** bhv Software	75,1
3	**Anti-Trojan Shield 2.2** Atshield	74,8
4	**Ewido Security Suite Free** Ewido Networks	73,0
5	**Trojan Hunter 3.9** Mischel Internet Security	71,7

Produkte im Detail

Ein Trojanerscanner muss sich daran messen lassen, wie gut es ihm gelingt, Spionageprogramme auf der Festplatte zu identifizieren. Darunter fallen zunächst die klassischen Trojaner, speziell die Remote-Access-Tools. Hier bieten einige Programme gute Leistungen. Die Spitze markiert Trojan Defence Suite, es setzt sich sogar von Norton Antivirus 2004 ab. Als einziges Programm verursacht Ewido Fehlalarme: Es deklariert Teile von T-Online 5.0 als Trojaner.

Probleme bei der Erkennung aktueller Viren und Würmer mit Backdoor-Funktion haben alle Trojanerscanner, mit Ausnahme von Trojan Defence Suite 3. Bei diesen Erkennungsraten zieht Norton Antivirus am gesamten Testfeld vorbei, es erkennt schlicht alle Schädlinge im Test. Eine sehr weit gefasste Definition für »schädliche Dateien« verwendet Spionage-Abwehr. Das Tool unterscheidet rund 40 Kategorien, zum Beispiel auch Scherzprogramme oder Dokumente über die Herstellung von Sprengstoff. Die Suche kann der Anwender für jede Kategorie einzeln ein- oder ausschalten. Für Firmen ist das sinnvoll, denn sie sind für die Dateien auf den PCs der Mitarbeiter verantwortlich.

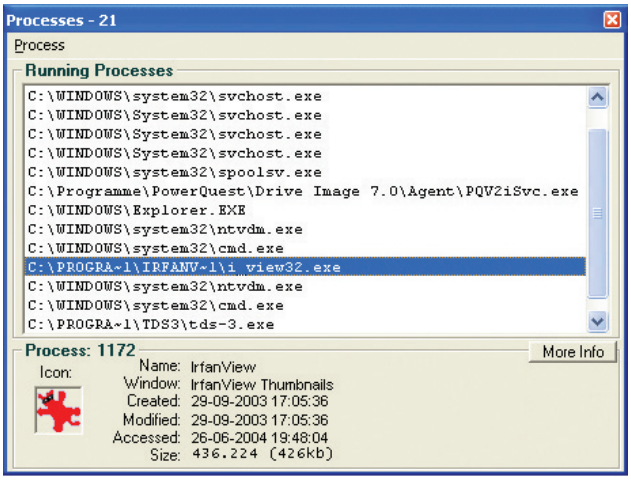
Die meisten Trojanerscanner können keine oder nur sehr wenige Archive durchsuchen. In dieser Disziplin sind Antivirenprogramme die bessere Wahl, das können diese nämlich alle.

Automatische Online-Updates

Wie Antivirenprogramme arbeiten die Trojanerscanner allesamt mit Signaturen, verfügen also über eine Datenbank mit »Fingerabdrücken« der Schädlinge. Nur Trojaner aus dieser Datenbank erkennen sie sicher. Deshalb sind regelmäßige Online-Updates obligatorisch. Alle Programme besitzen diese Option. Anwender müssen aber die Online-Prüfung bei einigen Tools wie Digital Patrol oder Tauscan umständlich selbst starten, der Scanner bleibt von sich aus untätig.

Autostart & Co

Habne Sie den Verdacht, ein bisher unbekannter Trojaner habe sich auf dem PC eingenistet, müssen Sie die laufenden Prozesse prüfen: Im Gegensatz zu den meisten Virenscannern bieten Trojanerjäger wie TDS 3 dafür eine Liste der aktiven Prozesse. Genauso wichtig ist ein Blick auf die verstreuten Autostart-Varianten. Auch das können Trojanerscanner besser als Virenscanner. Damit ein Trojaner bei Systemstart aktiv wird, muss er sich dort eintragen (siehe »Know-how: Kriminelle Tools«, Seite 127).

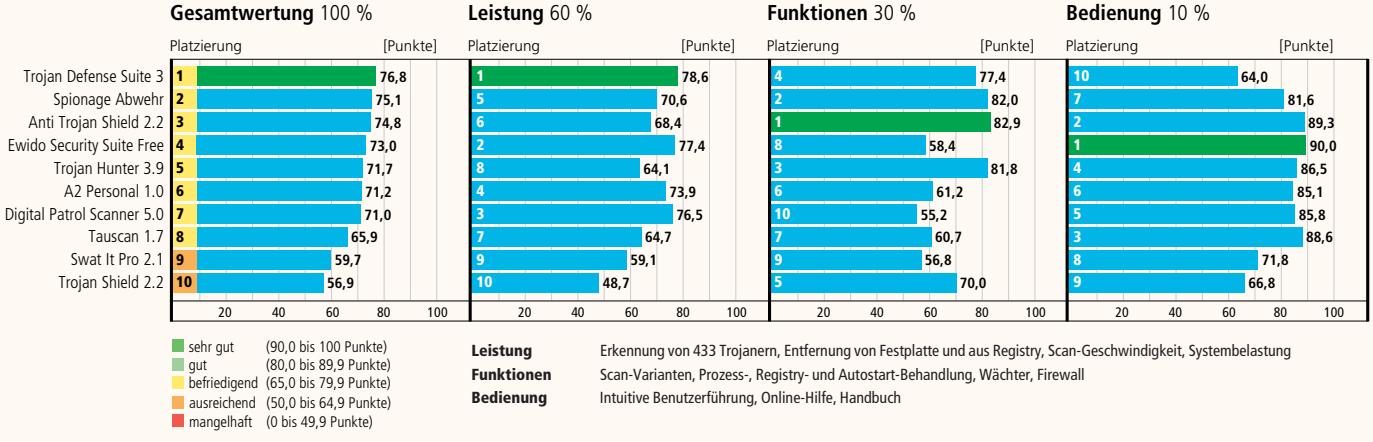


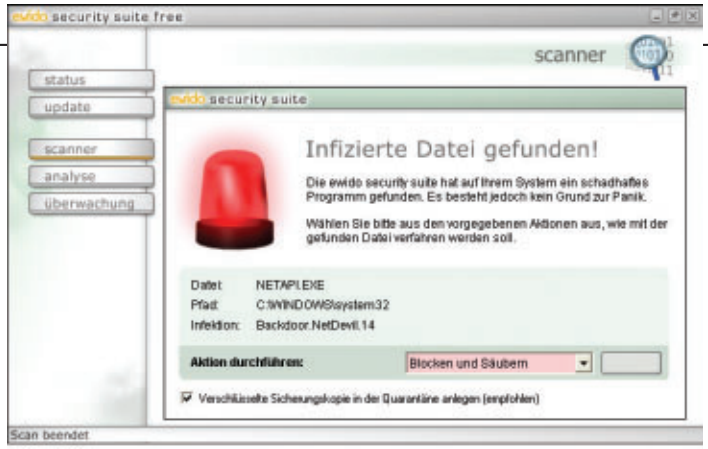
Die Liste laufender Prozesse zeigt bei Trojan Defence Suite auch den genauen Pfad der Programmdatei an.

Nicht im Test

Die Trojanerscanner Trojan Guarder *(www.anti-viruses.net)*, Sentinel *(www.runtimeware.com)*, PC Doorguard *(www.astonsoft.com)* und The Cleaner Professional *(www.moosoft.com)* nehmen nicht am Test teil, weil die Hersteller keine Vollversionen zur Verfügung stellen. BO Clean *(www.nsclean.com)* enthält keinen Scanner, sondern nur einen Wächter. Ewido Security Suite und A2 sollen demnächst in neuen Versionen erscheinen, getestet werden die bis Redaktionsschluss aktuellen Versionen.

Wertungen & Messwerte





Ewido Security Suite Free blockiert gefundene Schädlinge und reinigt die infizierten Dateien.

Weitere Infos

- **isc.sans.org**
  Das Internet Storm Center: Top-Adresse mit Meldungen über aktuelle Bedrohungen, Funktionsweise von Angriffen, Sicherheitslücken inklusive Lösungen, Hintergrund-Papers und anderem
- **www.cert.org**
  Ähnlich wie ISC, erste Anlaufstelle bei Sicherheitsproblemen
- **www.bsi.de**
  Bundesamt für Sicherheit in der Informationstechnik, bietet aktuelle und ausführliche Informationen, einige Artikel speziell für unerfahrene Anwender
- **www.trojaner-info.de**
  Sehr gute deutsche Seite mit vielen Informationen zu Sicherheitsthemen

Prozesse beenden

Geradezu lebenswichtig für die Diagnose ist eine Liste der geöffneten Ports mit den zugeordneten Programmen. Alle Tools bis auf Spionage-Abwehr, Tauscan oder Digital Patrol können das. Die Angabe des kompletten Pfads zur Programmdatei erleichtert die Unterscheidung zwischen eigenen und schädlichen Programmen. Verdächtige Prozesse werden über die Prozessliste beendet. Aber das versuchen manche Trojaner und Würmer nach Kräften zu verhindern. So starten sie wie W32/Prettypark mehrere Prozesse, die sich gegenseitig überwachen. Wird ein Prozess beendet, so startet der verbliebene Prozess sofort einen neuen. Spionage-Abwehr hat damit erhebliche Probleme. So meldet es zwar immer wieder einen laufenden Prozess von Prettypark und Bionet, konnte diese aber nicht beenden. Letztlich muss man sie vom Scanner ignorieren lassen und einen anderen Trojanerjäger benutzen. Bei einer Durchsuchung der Festplatte löscht Spionage-Abwehr aber dann die beiden Dateien, ein Windows-Neustart entfernt sie aus dem Speicher.

Trojan Shield bringen die eingeschleusten Trojaner völlig aus dem Tritt: Auf dem infizierten Testsystem lässt sich das Tool nicht vollständig installieren, denn beim Neustart bleibt Windows hängen. Tauscan stürzt bei dem Versuch, den Trojaner Theefle zu beenden, ab. Alle anderen Scanner können Prozesse beenden.

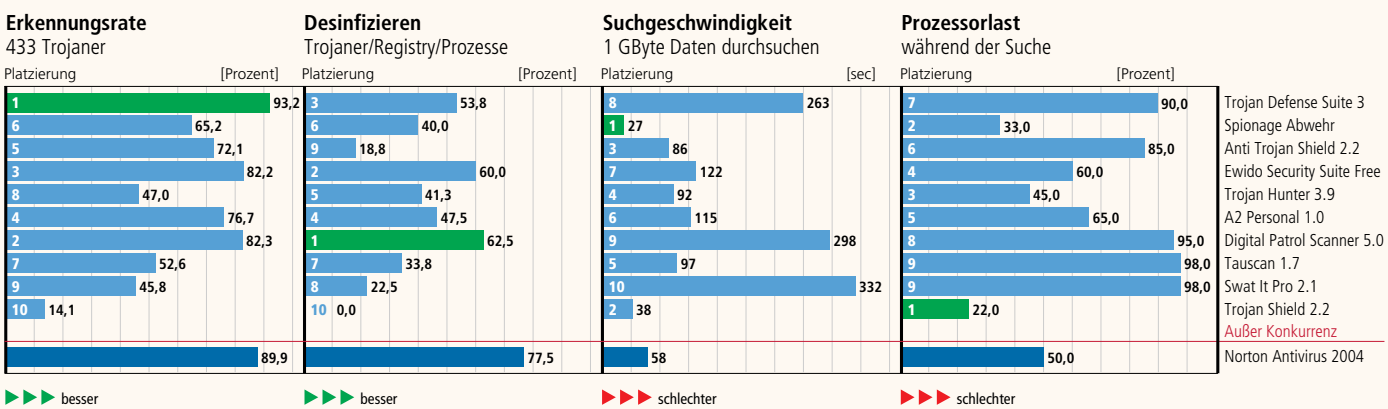
System reinigen

Laufende Prozesse stellen auch ein Problem für das Löschen von Dateien dar. Denn Windows NT, 2000 und XP sperren den Zugriff auf die zugehörigen Programmdateien. Digital Patrol Scanner löst das Problem durch einen Windows-Neustart. Der Löschvorgang erfolgt während des Starts von Windows, während die Prozesse noch nicht aktiv sind. Tauscan fordert ebenfalls einen Windows-Neustart an, danach muss der Anwender aber von Hand einen Scan der Festplatte starten.

Viele Trojaner erzeugen nicht nur eine Datei auf der Festplatte, sondern gleich mehrere. Im Löschtest sollen die Trojanerscanner deshalb insgesamt 32 Dateien und Verzeichnisse auf Laufwerk C aufspüren und entfernen. Vollständig schafft das kein Programm im Test. Mit 26 oder mehr entdeckten und beseitigten Dateien schneiden A2 Personal, Digital Patrol, Ewido Security Suite Free und Trojan Defence Suite noch relativ gut ab. Die Spitze mit 30 gelöschten Dateien markiert aber Norton Antivirus 2004.

Auch die Autostart-Einträge in der Registry sollte der Scanner entfernen. Zwar ist ein Registry-Eintrag ungefährlich, wenn die zugehörige Programmdatei gelöscht ist, doch irritieren solche Reste etwa bei der Kontrolle der Autostart-Liste. Am besten schneiden hier Ewido Security Suite, Spionage-Abwehr und Trojan Hunter ab.

Die Probanden verhalten sich sehr unterschiedlich. TDS 3 erkennt zwar am meisten, reinigt aber schlecht, ist langsam und schwer bedienbar. BMU



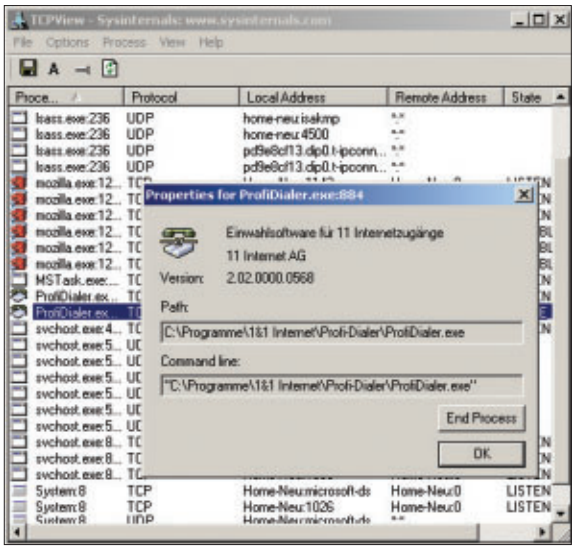
Know-how – Spione enttarnen

Mit Bordmitteln von Windows und Freeware-Tools entdecken Sie die meisten Trojaner. Mit dem richtigen Know-how spüren Sie verdächtige Prozesse im Speicher auf und erhalten so Informationen über den Zustand Ihres Systems. Wolfgang Nefzger

Das Wichtigste für einen Trojaner ist es, möglichst lange unentdeckt zu bleiben.

Jeder PC sollte mit einer Desktop-Firewall ausgestattet sein, zum Beispiel mit der Sygate Personal Firewall 5.5 (Testsieger in *PC Professionell* 3/2004, Seite 118). Diese blockt unerlaubte Zugriffe von außen. Damit haben Würmer wie Mydoom oder Sasser keine Chance. Die Firewall akzeptiert nur solche Datenpakete, die als Antwort auf die Anfrage eines Programms zurückkommen. Öffnet ein Trojanerprogramm eine Backdoor, also einen bestimmten Port, so registriert die Firewall dies. Stellen Sie Ihre Firewall unbedingt so ein, dass Sie den Zugriff grundsätzlich persönlich freigeben müssen. Perfekt ist diese Lösung allerdings nicht. Es gibt Schädlinge wie Agobot (Phatbot), die gezielt versuchen, eine aktive Firewall auszuschalten. Gute Firewalls wie Sygate oder Norton lassen sich als Gegenwehr per Passwort schützen. Nur wer das Kennwort eintippt, darf die Firewall beenden.

Parallel dazu gibt es deshalb Programmtricks, um die Firewall zu umgehen. Der Trojaner kann beispielsweise seine Datenpakete als HTTP-Kommunikation über Port 80 tarnen.



Gute Kontrolle: Mit TCP-View von Sysinternals sehen Sie, welche Verbindungen ein Programm geöffnet hat.

Die Daten übergibt der Trojaner dazu an den Browser (oder ein anderes Programm), das bei der Firewall keinen Verdacht erregt, weil es als legales Internet-Programm registriert ist.

Versteckte Prozesse mit Tools auflisten

Wenn ein Programm unter Windows ausgeführt wird, erscheint es in einer internen Liste, der Prozessliste. Ein Trojaner oder Wurm, der per Autostart aktiv wird, erscheint meistens, aber nicht immer, in der Prozessliste. Bei Windows NT/2000 und XP zeigen Sie diese Liste über den Taskmanager und das Register *Prozesse* an. Ein nützliches Tool mit zusätzlichen Funktionen ist Process Explorer von Sysinternals *(www.sysinternals.com)*. Damit sehen Sie zum Beispiel, auf welche anderen Dateien ein Prozess gerade zugreift.

Um sich zu verstecken, verwenden die Programmierer von Trojanern unverdächtige Dateinamen wie *winregsrv.exe* oder *files32.vxd*. Da die Prozessliste auf einem typischen PC 20 oder mehr Einträge hat, kann man nicht immer genau sagen, ob es sich dabei um schädliche Programme handelt. Nützliche Informationen zu den Prozessnamen finden sich am schnellsten über Suchmaschinen wie Google.

Jedes Programm, das auf das Internet zugreift, benutzt Ports für die Verbindungen. Diese zeigen Sie sich auf der Kommandozeile mit *netstat* an. Durch Vergleich mit bekannten Trojaner-Ports lassen sich so eventuell verdächtige Verbindungen erkennen. TCP-View von Sysinternals nennt zudem das Programm, das den Port geöffnet hat, und kann diese Anwendung auch beenden. BMU

Tools, die man haben muss

■ 75 Sicherheits-Tools
Bei Insecure.org finden Sie neben dem kostenlosen Portscanner NMap, der Sicherheitslücken im LAN aufspürt, auch eine Liste mit den laut einer Umfrage 75 besten Sicherheits-Tools für Windows und Linux *(www.insecure.org/tools.html)*.

■ Backdoors suchen
Die Betreiber der Site Sysinternals, Mark Russinovich und Bryce Cogswell, programmieren seit Jahren geniale System-Tools für Windows *(www.sysinternals.com)*. Die meisten Programme gibt es sowohl für Windows 98/Me als auch NT/2000/XP. Für die Backdoor-Suche sind Process Explorer, TCP-View, TDI-Mon und Autoruns besonders interessant.

■ Desktop-Firewall
Wenn Sie kein Geld für eine Firewall ausgeben wollen, gibt es reichlich kostenlose Angebote. Der Funktionsumfang ist zwar nicht überwältigend, die Grundfunktionen sind aber vorhanden. Sie finden kostenlose Desktop-Firewalls in aktuellen Versionen etwa bei Sygate *(www.sygate.de)*, Kerio *(www.kerio.com)* sowie Zonelabs *(www.zonelabs.com)*.

■ Portscanner
Mit dem kostenlosen Tool Fport listen Sie auf der Kommandozeile von Windows NT/2000/XP alle Ports auf, die geöffnet sind *(www.foundstone.com)*. Zu jedem Port zeigt das Sicherheits-Tool auch den zugehörigen Programmnamen und sogar den genauen Pfad der Programmdatei auf.

Know-how – Kriminelle Tools

Nur wer weiß, wie Trojaner und andere Backdoor-Schädlinge funktionieren, kann sie aufspüren und vernichten. Die Spionageprogramme gelangen auf vielen Wegen zu ihren Opfern und bieten sogar umfassende Konfigurationsoptionen. Wolfgang Nefzger

Eine Backdoor besteht aus zwei Komponenten: einem Server und einem Client. Auf dem PC des Opfers ist die Server-Komponente installiert. Diese öffnet einen Kanal zum Internet (Port), eine so genannte Backdoor. Über diesen Kanal empfängt der Server Kommandos vom Angreifer und führt diese aus. Als Übertragungskanal dient auch oft der Internet Relay Chat (IRC). Manche Server werden auch selbst aktiv und senden von sich aus Daten an bestimmte E-Mail- und IP-Adressen oder IRC-Kanäle. Diese Daten kann der Angreifer über ein Setup-Programm vor der Infektion einstellen.

Infektionswege

Der klassische Infektionsweg für einen Trojaner funktioniert noch immer: Mit einem Setup-Programm (auch Binder genannt) schleust der Angreifer den Server in ein beliebiges Programm ein, etwa ein kostenloses FTP-Programm. Dieses Tool steht dann in Newsgroups, auf Websites und FTP-Servern zum Download bereit. Sehr beliebt sind zur Verbreitung auch P2P-Netzwerke wie Kazaa. Installiert ein argloser Anwender das Programm, so verankert sich zunächst der Trojaner-Server im PC. Danach startet das Tool selbst, so dass der Anwender von der Infektion nichts bemerkt.

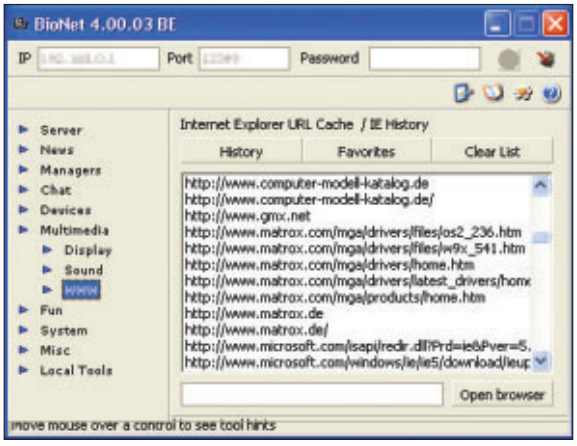
In jüngster Vergangenheit verstärkt sich der Trend, Backdoors auch durch Viren oder Würmer zu installieren. Bekannte Beispiele sind Mydoom, Sasser oder Kwbot. Solche Schädlinge verbreiten sich über Sicherheitslücken, verschicken E-Mails mit infiziertem Anhang oder kopieren sich automatisch in Kazaa-Tauschverzeichnisse.

Einmal auf dem PC, versucht der Server sich so zu verankern, dass er bei jedem Systemstart aktiv wird. Dazu gibt es eine Reihe von Möglichkeiten. Nähere Informationen finden Sie im Kasten »Gefährliche Autostarts«. Dabei versucht der Spion alles, um unentdeckt zu bleiben.

Das Gegenstück zum Server ist der Client auf dem PC des Angreifers. Das ist ein normales Windows-Programm mit Hauptfenster, in dem der Angreifer eine Reihe von Kommandos aufrufen kann. Das Fernsteuern fremder PCs sollte stets auf Rechner beschränkt bleiben, für die man Zugriffsrechte hat, es gilt sonst als Computer-Kriminalität.

Verbotene Funktionen

Exemplarisch sei im Folgenden auf die Backdoor Bionet 4.0 näher eingegangen. Unter der Kategorie *Server* konfiguriert der Angreifer den Server auf dem anderen PC, sogar ein Online-Update der Server-Komponenten ist vorgesehen. Außerdem darf der Angreifer Programme auf den Opfer-PC laden und dort installieren.



Das Client-Programm des Trojaners Bionet bietet erstaunliche Funktionsvielfalt. Hier zeigt es die zuletzt aufgerufenen Web-Adressen an.

Die Rubrik *Manager* ist das Herzstück von Bionet. Mit dem *File Manager* greift der Hacker auf die Festplatte des Opfers zu und erzeugt oder löscht Dateien und Ordner. Auch ein Dateitransfer vom und zum Client-PC ist kein Problem. Der *Window Manager* gibt Auskunft, welche Fenster auf dem Opfer-PC gerade geöffnet sind.

Diese beispielhaften Funktionen zeigen, wie wichtig ein guter Schutz des eigenen PCs durch Antiviren- oder Anti-Trojaner-Programme ist. BMU

Gefährliche Autostarts

Windows bietet Programmen eine Reihe von Optionen, damit diese beim Systemstart automatisch aktiv werden. Das nutzen auch Trojaner und Würmer aus. Anwender sollten die entsprechenden Autostart-Einträge regelmäßig gründlich überprüfen.

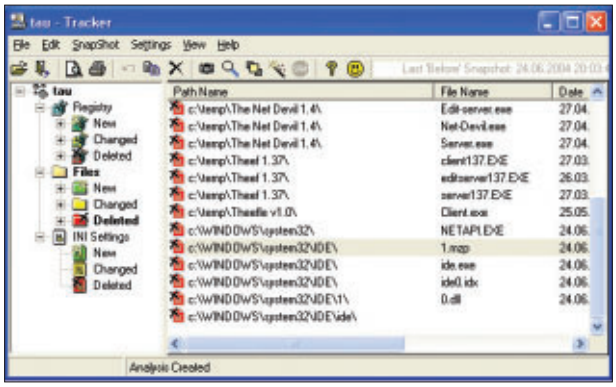
- Der Autostart-Ordner im Startmenü ist die offensichtliche Lösung, aber sehr leicht zu durchschauen.
- Die Textdateien *win.ini* und *system.ini* enthalten Einträge, die Programme starten. Achten Sie auf die Zeilen, die mit *load=* oder *run=* oder *shell=* (nur bei Windows 95/98/Me vorhanden) beginnen.
- Die Registry enthält in mehreren Schlüsseln Einträge für Autostart-Programme:
  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- Eine raffinierte Methode ändert das Standardverhalten von Windows beim Doppelklick auf eine Datei. EXE-Dateien werden dadurch normalerweise gestartet. Backdoors wie W32/Prettypark ändern den Eintrag so, dass jedes Mal zunächst der Wurm und dann erst das angeklickte Programm startet: *HKEY_CLASSES_ROOT\exefile\shell\open\command* und *HKEY_LOCAL_MACHINE\Software\Classes\exefile\shell\open\command*.

Einen schnellen Überblick über die verschiedenen Autostart-Einträge in der Registry verschaffen Sie sich mit dem Tool *Autoruns* von Sysinternals *(www.sysinternals.com)*.

So testet PC Professionell

Die Anti-Trojaner-Software muss im Test an zwei Fronten ihre Wirksamkeit beweisen. Zum einen stellen die Laborexperten die Tools mit 433 verbreiteten Trojanern, Viren und Würmern mit Backdoor-Funktion auf die Probe. Zum anderen müssen die Tools einen entsprechend infizierten PC säubern.

Der Scanner sucht primär infizierte Dateien auf der Festplatte. Im Test müssen die Tools 210 Backdoor-Clients (Steuerungssoftware für Angreifer) und 192 Backdoor-Server (versteckte Programme auf dem Opfer-PC) entdecken. In jüngster Zeit rücken verstärkt



Das Snapshot-Programm Tracker protokolliert genau, welche Dateien und Registry-Einträge die Trojanerscanner bereinigt haben.

Würmer und Viren mit Backdoor-Funktionalität wie Mydoom oder Sdbot in den Vordergrund. 25 verbreitete Vertreter dieser Gattungen sollen die Scanner entdecken. Dazu kommen noch sechs verschiedene Angriffstools wie Keylogger.

Um abzuschätzen, wie schnell die Scanner arbeiten, müssen diese 7100 Dateien mit insgesamt 960 MByte Umfang durchsuchen. Darin sind keine Archive enthalten, um das Ergebnis nicht zu verfälschen, denn einige Trojanerscanner können keine Archive durchsuchen.

Ein zweiter wichtiger Bereich ist das Säubern eines infizierten Systems. Dazu verseuchen die Tester einen PC mit acht besonders gefährlichen Trojanern und Backdoor-Würmern. Die Tools müssen zum einen die laufenden Trojanerprozesse entdecken und beenden. Dann durchsuchen die Scanner das Systemlaufwerk C, auf dem die Trojaner insgesamt 32 Dateien angelegt haben. Diese sollen entdeckt und gelöscht werden. Auch in der Registry haben sich die Spione an zwölf verschiedenen Stellen eingetragen. Das Snapshot-Programm Tracker protokolliert genau die Änderungen an Dateien und der Registry.

Testaufbau

Prozessor: Athlon XP/1,8 GHz • Arbeitsspeicher: 256 MByte RAM • Festplatte: 120 GByte • Online-Verbindung: ISDN • Betriebssystem: Windows XP Home SP 1

Wertung & Ausstattung

PLATZ ①

PC Professionell Empfehlung der Redaktion

TDS-3 PROFESSIONAL

Produkt		**Trojan Defence Suite 3**
Hersteller		**Diamond Computer Systems**
Gesamturteil	[Punkte]	**befriedigend 76,8**
Leistung (60 %)	[Punkte]	2. Platz 78,6
Funktionen (30 %)	[Punkte]	4. Platz 77,4
Bedienung (10 %)	[Punkte]	11. Platz 64,0
Info		tds.diamondcs.com.au
Internet		tds.diamondcs.com.au
Preis		40 Euro
Sprache		Englisch
Ausstattung Scanner		
Scannt Dateitypen		●
Scannt alle Dateien		●
Scannt einzelne Verzeichnisse		●
Scannt NTFS-Datastreams		●
Ausnahmenliste		●
Scannt Archive		●
Scannt Mail-Datenbanken		○
Scannt Arbeitsspeicher		●
Scannt Registry		●
Scannt INI-Dateien		●
Scannt Ports		●
Heuristik		●
Anzeige Autostart-Registry		●
Anzeige Autostart-Ordner		●
Anzeige Autostart über Datei		●
Anzeige aktiver Prozesse		●
Prozess beenden		●
Anzeige aktiver Fenster		●
Anzeige offene Ports TCP/UDP		●/●
Ausstattung Wächter		
Wächter vorhanden		○
Integrierte Firewall		○
Prüft aktive Prozesse		○
Prüft Registry-Zugriffe		○
Prüft Internet-Zugriffe		○
Prüft neue Dateien		○
Prüft Programme vor Start		●[3)]
Benutzeroberfläche		
Quarantäne		○
Sicherheitskopie vor Reinigung		○
Zeitplaner		○
Schädlingsliste		●
Liste Trojaner-Ports		●
Logdateien		●
Zugriff über Kontextmenü		●
Sonstige Ausstattung/Support		
Erkennt Dialer/Spyware		●/○
Online-Hilfe		●
Gedrucktes Handbuch		○
Sonstiges		integrierte Skriptsprache, Schnittstelle für Plug-ins, Integritäts-Checker
Online-Update		●
Update-Frequenz (Herstellerangabe)		täglich
Automatische Updates		○
Hotline		Webformular
Fazit		sehr gute Suchleistung und viele Funktionen, es fehlt aber ein Hintergrundwächter

● = ja ○ = nein k. A. = keine Angabe

	PLATZ ②	PLATZ ③	PLATZ ④	PLATZ ⑤	PLATZ ⑥
					
	Spionage-Abwehr	**Anti-Trojan Shield 2.2**	**Ewido Security Suite Free**	**Trojan Hunter 3.9**	**A2 Personal 1.0**
	bhv Software	**Atshield**	**Ewido Networks**	**Mischel Internet Security**	**Emsi Software**
	befriedigend 75,1	**befriedigend 74,8**	**befriedigend 73,0**	**befriedigend 71,7**	**befriedigend 71,2**
	6. Platz 70,6	7. Platz 68,4	3. Platz 77,4	9. Platz 64,1	5. Platz 73,9
	2. Platz 82,0	1. Platz 82,9	10. Platz 58,4	3. Platz 81,8	8. Platz 61,2
	8. Platz 81,6	3. Platz 89,3	2. Platz 90,0	5. Platz 86,5	7. Platz 85,1
	(021 31) 765 01	(+1) 372 51 92 79 21[1]	www.ewido.net/de	www.trojanhunter.com	(+43) 66 43 44 60 68[1]
	www.bhv.de	www.atshield.com	www.ewido.net/de	www.trojanhunter.com	www.emsisoft.de
	40 Euro	24 Euro	kostenlos	32 Euro	30 Euro
	Deutsch	Englisch	Deutsch	Englisch	Deutsch
	●	●	●	●	●
	●	●	●	●	●
	●	●	●	●	●
	○	●	○	●	○
	●	○	○	●	○
	●	●	○	●	●
	○	○	○	○	○
	●	●	○	●	●
	●	●	○	●	●
	●	●	○	●	●
	○	○	○	●	○
	●	●	○	●	○
	●	●	●	●	○
	○	●	●	●	○
	○	●	○	●	○
	●	●	●	●	●
	○	●	●	●	●
	○	●	○	●	○
	○/○	●/●	●/●	●/●	○/○
	●	●	○	●	○
	○	○	○	○	○[2]
	●	○	○	●	○
	●	○	○	○	○
	●	○	○	○	○
	●	●	○	○	○
	○	●	○	○	●
	●	●	●	○	○
	●	○	●	●	○
	○	●	○	○	○
	●	○	○	●	○
	○	○	○	●	○
	●	●	●	●	●
	●	●	●	●	●
	●/●	○/○	●/●	●/○	●/●
	●	●	●	●	○
	● 64 Seiten	○	○	○	○
	Cookie-Überwachung	○	Datei-Shredder, Sandbox zur Umgebung von Pack-Algorithmen, XP-AntiSpy	erweiterbar um eigene Such- und Löschregeln	IDS prüft live aktive Prozesse auf verdächtiges Verhalten
	●	●	●	●	●
	k. A.	k. A.	täglich	2–5 pro Woche	täglich
	○	○	○	●	○
	(08 00) 248 46 85[4]	support@atshield.com	support@ewido.net	support@misec.net	info@emsisoft.com
	Komplettpaket mit mäßiger Leistung und magerer Entfernungsrate	gute Suchleistung, aber schwach beim Entfernen aktiver Trojaner	brauchbare Suchleistung, ein Virenwächter kommt erst mit der nächsten Version	schwache Suchleistung bei Backdoor-Clients, sonst durchaus brauchbar	mäßige Suchleistung und recht wenig interessante Funktionen

[1] Auslandstarif [2] keine herkömmliche Desktop-Firewall, sondern nur Kontrolle über Ports, keine Filterung von eingehenden TCP-Paketen
[3] wenn Execution Protection bei aktivem Hauptprogramm eingeschaltet ist [4] gebührenfrei

Wertung & Ausstattung

		PLATZ ⑦	PLATZ ⑧	PLATZ ⑨	PLATZ ⑩
Produkt		**Digital Patrol Scanner 5.0**	**Tauscan 1.7**	**Swat It Pro 2.1**	**Trojan Shield 2.2**
Hersteller		**Proantivirus Lab**	**Agnitum**	**SwatIt.org**	**Trojanshield.com**
Gesamturteil	[Punkte]	**befriedigend 71,0**	**befriedigend 65,9**	**ausreichend 59,7**	**ausreichend 56,9**
Leistung (60 %)	[Punkte]	4. Platz 76,5	8. Platz 64,7	10. Platz 59,1	12. Platz 48,7
Funktionen (30 %)	[Punkte]	12. Platz 55,2	9. Platz 60,7	11. Platz 56,8	5. Platz 70,0
Bedienung (10 %)	[Punkte]	6. Platz 85,8	4. Platz 88,6	9. Platz 71,8	10. Platz 66,8
Info		www.antiviraldp.com	www.tauscan.com	(+60) 37 40 45 90[1)]	(02 21) 31 08 82
Internet		www.antiviraldp.com	www.tauscan.com	swatit.org	www.trojanshield.com
Preis		23 Euro	24 Euro	32 Euro	29 Euro
Sprache		Englisch	Englisch	Englisch	Englisch
Ausstattung Scanner					
Scannt Dateitypen		●	●	●	●
Scannt alle Dateien		○	●	○	●
Scannt einzelne Verzeichnisse		●	●	●	●
Scannt NTFS-Datastreams		○	○	○	○
Ausnahmenliste		○	○	○	●
Scannt Archive		●	●	●	○
Scannt Mail-Datenbanken		● The Bat, PlainMail, Outlook Express 4.x und 6.x	○	○	○
Scannt Arbeitsspeicher		●	●	○	●
Scannt Registry		○	○	○	○
Scannt INI-Dateien		○	○	○	○
Scannt Ports		○	○	○	○
Heuristik		○	●	○	○
Anzeige Autostart-Registry		●	○	●	●
Anzeige Autostart-Ordner		●	○	●	○
Anzeige Autostart über Datei		●	○	○	○
Anzeige aktiver Prozesse		○	○	●	●
Prozess beenden		○	○	●	●
Anzeige aktiver Fenster		○	○	○	○
Anzeige offene Ports TCP/UDP		○/○	○/○	●/●	○/○
Ausstattung Wächter					
Wächter vorhanden		○	●	○	●
Integrierte Firewall		○	○	○	○
Prüft aktive Prozesse		○	●	○	●
Prüft Registry-Zugriffe		○	○	○	○
Prüft Internet-Zugriffe		○	○	○	●
Prüft neue Dateien		○	○	○	○
Prüft Programme vor Start		○	○	○	○
Benutzeroberfläche					
Quarantäne		●	○	●	○
Sicherheitskopie vor Reinigung		○	●	○	○
Zeitplaner		○	○	●	○
Schädlingsliste		○	●	○	●
Liste Trojaner-Ports		○	○	○	○
Logdateien		●	●	●	●
Zugriff über Kontextmenü		○	●	○	○
Sonstige Ausstattung/Support					
Erkennt Dialer/Spyware		●/●	○/○	○/○	●/●
Online-Hilfe		●	●	○	●
Gedrucktes Handbuch		○	○	○	○
Sonstiges		○	○	○	Emulation für Trojaner-Server, Protokoll der Zugriffsversuche
Online-Update		●	●	●	●
Update-Frequenz (Herstellerangabe)		täglich	k. A.	täglich	k. A.
Automatische Updates		●	●	●	○
Hotline		support@antiviraldp.com	Webformular	(+60) 37 40 56 66[1)]	support@trojanshield.com
Fazit		gute Suchleistung, es fehlen aber ein Wächter und etliche andere Funktionen	gute Suchleistung bei klassischen RATs, aber wenig Funktionen	deutliche Schwächen bei der Suchleistung und der Geschwindigkeit	die Suchleistung von Trojan Shield kann in keiner Weise überzeugen

● = ja ○ = nein k. A. = keine Angabe [1)]Auslandstarif