INTERNET: Trojaner und Rootkits

Trojaner und Rootkits jagen

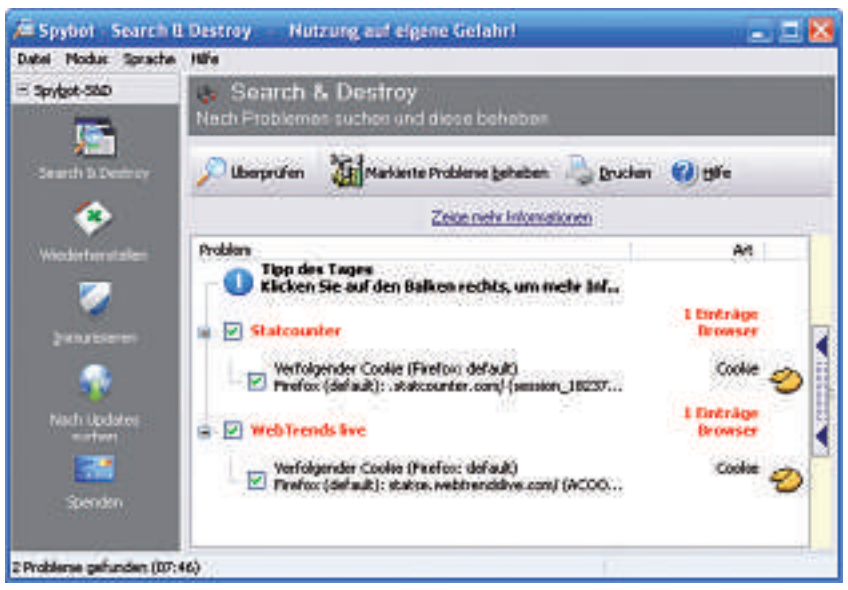
So spüren Sie verborgene Trojaner und unsichtbare Rootkits auf Ihrem Computer auf. Neue Reinigungs-Tools entfernen die Schädlinge zuverlässig.

Trojaner schleichen sich mit besonders fiesen Tricks auf fremden PCs ein. Oft tarnen sie sich als vermeintlich harmloses Programm oder Dokument – versendet von Kriminellen per Spam-Mail. Andere Trojaner verbreiten sich unauffällig über manipulierte Werbebanner, die gelegentlich auch auf seriösen Webseiten zu finden sind und Sicherheitslücken im Browser auszunutzen versuchen.

Die Betrüger greifen zu allen Mitteln: So haben sie ihre Schadprogramme schon als Windows-Update getarnt, als Rechnung, Mahnung oder Lotteriegewinn, als kostenlosen Codec zum Abspielen von Filmen und sogar als Sicherheits-Tool. In Wahrheit verbirgt sich unter der harmlosen Oberfläche jedoch ein gefährliches Schadprogramm, das weiteren Infektionen eines Computers Tür und Tor öffnet.

Sicherheitsexperten nennen einen Trojaner, der einen PC verseucht und weitere Schadsoftware nachlädt, einen Dropper. Das Wort stammt vom englischen Verb “to drop”, was auf Deutsch “fallen lassen” bedeutet. Die zusätzlichen Schädlinge öffnen meist eine Hintertür (englisch: Backdoor) auf dem PC, protokollieren Tastatureingaben (englisch: Keylogger) und erstellen Screenshots von Bildschirminhalten und versenden diese über das Internet.

Eine der gefährlichsten Schädlingsarten sind Rootkits. Nicht weil sie prinzipiell andere Funktionen als Trojaner oder Backdoor-Programme hätten, sondern weil sie sich so tief im System verankern, dass sie für Windows und für viele Virenscanner nicht mehr zu sehen sind.



Spybot 1.6.0: Wenn das Tool statt echter Spyware nur “verfolgende Cookies” findet, besteht keine Gefahr.

Trojaner und Rootkits aufspüren

Ein Schädling kommt selten allein. Die meisten aktuellen Trojaner laden weitere Malware herunter. Es ist deswegen notwendig, auf dem PC nicht nur nach Trojanern, sondern auch nach Spy- und Adware sowie nach Rootkits zu suchen.

Trojaner jagen

Trojan Hunter 5.0 (40 Dollar, eingeschränkte 30-Tage-Demo unter **www.misec.net/trojanhunter** und auf der Heft-CD) ist auf die Jagd nach Trojanern spezialisiert. Das Programm untersucht nicht nur sämtliche Dateien auf der Festplatte, sondern prüft auch den Arbeitsspeicher, die Registrierungsdatenbank und alle geöffneten Ports.

Mit der 30-Tage-Demo von Trojan Hunter lassen sich Trojaner aufspüren, allerdings nicht entfernen. Aufgrund der guten Erkennung eignet sich Trojan Hunter jedoch trotzdem zur Suche nach Trojanern.

Verwenden Sie zum Entfernen der Übeltäter dann die Freeware-Tools, die der Abschnitt “Reinigungs-Tools gegen Trojaner” beschreibt.

So geht’s: Starten Sie das Setup von Trojan Hunter. Klicken Sie auf *Next*, wählen Sie *I accept the agreement* aus und bestätigen Sie danach zwei Mal mit *Next*. Schliessen Sie die Installation mit einem Klick auf *Finish* ab, starten Sie das Programm aber noch nicht.

Aktualisieren Sie zuerst die Signaturen. Laden Sie dazu die Datei *http://www2.misec.net/rulefiles/zip/Update.zip* herunter und entpacken Sie ihren Inhalt in den Unterordner *Rule Files* im Installationsordner von Trojan Hunter, meist ist dies *C:\Programme\TrojanHunter 5.0*.

Optimieren Sie als Nächstes die Einstellungen des Programms. Starten Sie Trojan Hunter und klicken Sie dann links unten auf *Options*. Setzen Sie je ein Häkchen in die Kästchen vor *Enable script checker*, *Warn on runtime-packed files that cannot be unpacked* und *Warn on executable files with double extensions*.

Starten Sie Ihren PC nun im abgesicherten Modus neu. Drücken Sie dazu mehrmals die Taste *[F8]*, bevor das Windows-Logo wieder erscheint. Wählen Sie aus dem Bootmenü *Abgesicherter Modus* aus und bestätigen Sie mit der *Eingabetaste*.

Nachdem Windows fertig gestartet ist, rufen Sie Trojan Hunter auf und klicken auf *Full Scan*. Die Überprüfung dauert je nach Grösse der Festplatte bis zu einer Stunde. Gefundene Schädlinge zeigt das Tool im Feld *Scan Report* an. Dieser Teil des Fensters lässt sich nicht grösser ziehen, so dass man die Liste mit den Pfeiltasten durchgehen muss.

Nach dem Scan fordert Trojan Hunter Sie auf, die Vollversion zu erwerben, um gefundene Schädlinge auch zu entfernen. Das ist jedoch nicht nötig. Probieren Sie erst die Freeware-Programme aus dem Abschnitt “Reinigungs-Tools gegen Trojaner” aus. Klicken Sie deshalb auf *No* und rufen Sie danach *File, Save Scan Report* auf. Sichern Sie den Bericht.

Sobald Sie die Programme eingesetzt haben, die die folgenden Abschnitte und der Abschnitt “Reinigungs-Tools gegen Trojaner” empfehlen, sollten Sie den Scan mit Trojan Hunter noch einmal durchführen.

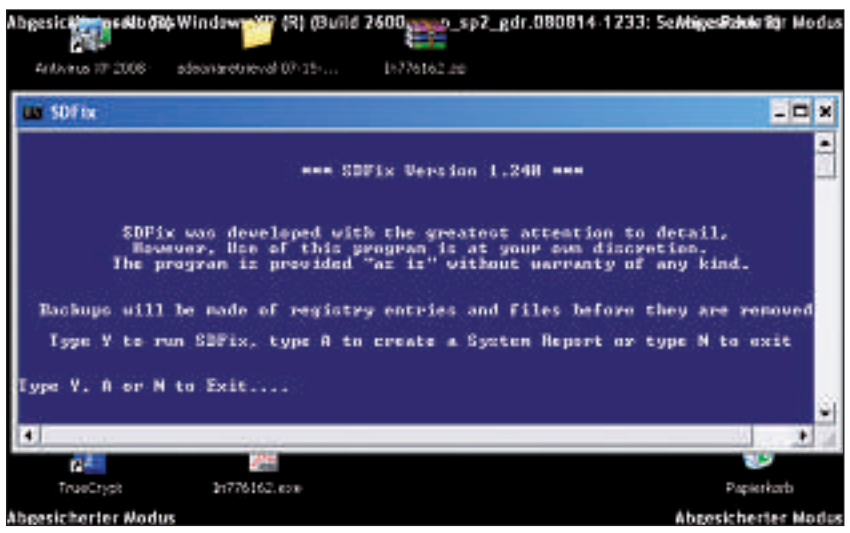
Falls dann immer noch Trojaner gefunden werden, geben Sie die Namen der Schädlinge bei Google ein. Eventuell finden Sie zur Bereinigung ein spezielles Removal-Tool von einem der grossen Antivirenhersteller oder auch Tipps in Foren.

Spyware jagen

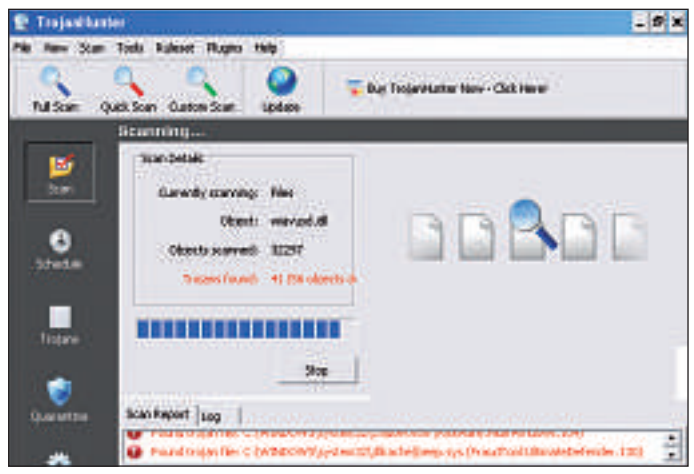
Spy- und Adware landet oft im Zuge einer PC-Infektion mit einem Trojaner auf der Festplatte. Spybot Search & Destroy 1.6.0 (kostenlos, **www.safer-networking.org/de/spybotsd** und auf der Heft-CD) ist ein bewährtes Programm, das viele Werbe- und Spionage-Tools erkennt und entfernt.

So geht’s: Führen Sie das Setup von Spybot Search & Destroy durch. Bei einer aktiven Internetverbindung lädt das Programm während der Installation automatisch die aktuellen Spyware-Signaturen herunter.

Beim ersten Start öffnet Spybot einen Assistenten, mit dem Sie eine Sicherung der Registrierungsdatenbank anlegen und Ihren PC “immuni-



SD Fix 1.240: Die Jagd nach Trojanern ist im abgesicherten Modus am effektivsten, weil sich die Übeltäter dann nicht schützen können.



Scan mit Trojan Hunter: Bei der Suche nach Trojanern und anderen Schädlingen im abgesicherten Modus lässt sich das Feld “Scan Report” nicht grösser ziehen.