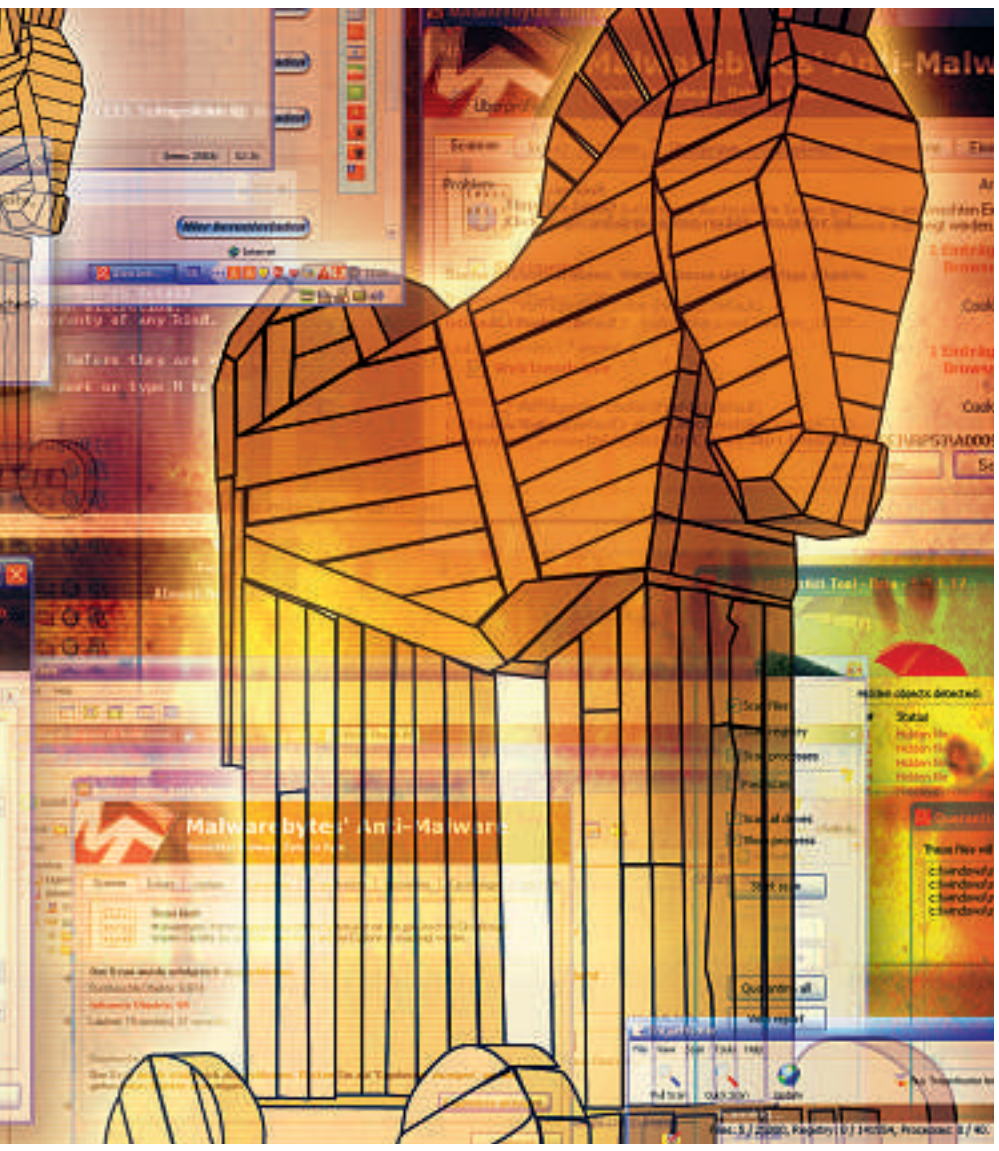


Trojan Hunter 5.0: So sehen die optimalen Scan-Einstellungen für das Anti-Trojaner-Tool aus.

sieren". Dabei fügt das Programm eine umfangreiche Liste gefährlicher Webseiten in die Hosts-Datei auf Ihrem PC ein. Diese Seiten werden dann geblockt.

Mit einem Klick auf *Überprüfen* starten Sie die eigentliche Suche nach Spyware. Entfernen Sie nach dem Scan alle gefundenen Bedrohungen mit *Markierte Probleme beheben*. Wenn nur "verfolgende Cookies" (englisch: Tracking Cookies) gefunden wurden, besteht kein Grund zur Sorge.

Rootkits jagen

Rootkits sind eine besonders bedrohliche Gefahr, weil sie nur mit speziellen Tools zu entdecken sind. Ein Rootkit verhindert mit einem eigenen Systemtreiber, dass es im Windows-Explorer angezeigt wird. So tarnen sich diese Schädlinge auch vor den meisten Antivirenprogrammen. Obwohl das Rootkit aktiv ist und in der Regel alle Funktionen eines Trojaners wie Backdoor und Keylogger hat, nimmt es der Virenscanner nicht wahr.

Ein Tool gegen Rootkits wie Avira Anti-Rootkit 1.0.1.17 (kostenlos, **www.free-av.de/de/tools/4/avira_antirootkit _tool.html** und auf der Heft-CD) vergleicht die Daten auf der Festplatte mit denen im Arbeitsspeicher und entdeckt und entfernt die heimlichen Schädlinge.

So geht's: Installieren Sie Avira Anti-Rootkit und starten Sie das Programm anschliessend über *Start*, *Avira Rootkit Detection*, *Avira Rootkit Detection*.

Klicken Sie auf *Start scan*. Eventuell gefundene Rootkits entfernen Sie anschliessend mit *Quarantine all* und zwei Mal *OK*. Ihr Rechner muss nun neu gestartet werden. Führen Sie die Suche nach Rootkits anschliessend noch einmal durch, um sicherzustellen, dass keine Vertreter dieser besonderen Schädlinge mehr vorhanden sind.

Reinigungs-Tools gegen Trojaner

Mit speziellen Reinigungsprogrammen entfernen Sie hartnäckige Trojaner von Ihrem Computer. Diese Tools verfügen bis auf Anti-Malware 1.32 über keine schicke Oberfläche, sondern sind ganz auf ihre Aufgabe hin optimiert: heimlichen Schädlingen den Garaus zu machen.

SD Fix 1.240

Die Freeware SD Fix 1.240 (kostenlos, **www.sdfix.net**) kennt und entfernt mehrere Hundert Trojaner. Ausserdem bereinigt das Programm die Windows-Registrierungsdatenbank von Malware-Einträgen.

So geht's: Starten Sie *SDFix.exe*, um die Software automatisch in den Ordner *C:\SDFix* auszupacken. Booten Sie anschliessend Ihren PC neu und drücken Sie – noch bevor das Windows-Logo erscheint – mehrmals *[F8]*. Sie sehen nun ein Bootmenü. Wählen Sie *Abgesicherter Modus* aus. Nur in diesem Modus bereinigt SD Fix Ihren Computer, weil Schädlinge sich so nicht aktivieren und ihren Selbstschutz nutzen können.

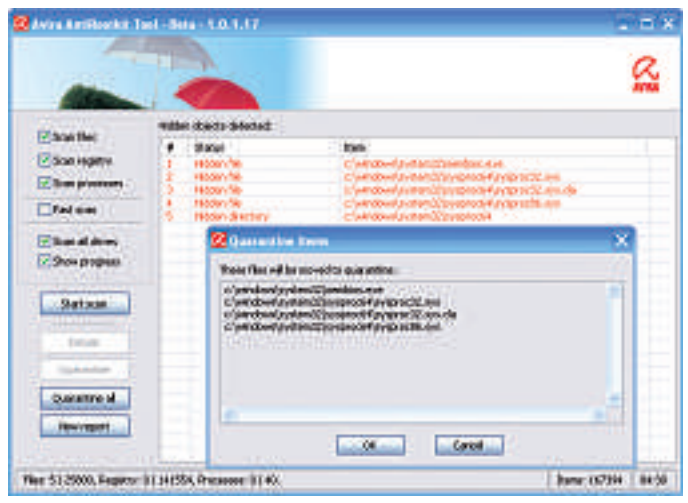
Sobald Windows im abgesicherten Modus läuft, drücken Sie *[Windows R]*, geben `C:\SDFix\RunThis.bat` ein und bestätigen mit *OK*. Ein blaues Fenster öffnet sich. Drücken Sie *[Y]*, um die Bereinigung zu starten, die je nach Festplatte eine Weile dauert. Drücken Sie eine beliebige Taste, wenn Sie von SD Fix dazu aufgefordert werden, um Ihren PC neu zu starten. Das Freeware-Tool führt anschliessend eine Bereinigung mit dem integrierten Anti-Rootkit-Tool Gmer (kostenlos, **www.gmer.net**) durch. Drücken Sie eine beliebige Taste, wenn der Check durchgelaufen ist. SD Fix öffnet danach einen Report im TXT-Format, der Informationen über gefundene und entfernte Schädlinge enthält.

Vundofix 7.0.6

Mit Vundo-Trojaner bezeichnen Sicherheitsexperten eine weit verbreitete Familie von Trojanern, die mit Pop-ups nervt und Werbung für verschiedene gefälschte Sicherheitsprogramme macht. Das Freeware-Tool Vundofix 7.0.6 (kostenlos, **http://vundofix.atribune.org**) ist auf die Entfernung dieser Trojaner spezialisiert.

So geht's: Rufen Sie die Seite http://vundofix.atribune.org auf und laden Sie das Reinigungs-Tool mit einem Klick auf *Download VundoFix* herunter. Starten Sie Vundofix anschliessend mit einem Doppelklick. Klicken Sie auf *Scan for Vundo*, um mit dem Check zu beginnen. Sobald der Vorgang abgeschlossen ist, entfernen Sie alle gefundenen Schädlinge mit *Fix Vundo* und *YES*.

Vundofix 7.0.6: Das Tool erkennt und entfernt die verbreiteten Trojaner der Vundo-Familie.



Avira Anti-Rootkit 1.0.1.17: Ein Klick auf "Quarantine all" entfernt gefundene Rootkits von Ihrem PC.

Anti-Malware 1.32

Anti-Malware 1.32 (kostenlos, **www.malwarebytes.org/mbam.php** und auf der Heft-CD) zählt zu den mächtigsten Reinigungs-Tools gegen Trojaner. Anders als die anderen beiden bereits vorgestellten Reinigungsprogramme arbeitet das Programm auch mit Signaturen.

So geht's: Führen Sie das gut dokumentierte Setup durch und aktualisieren Sie anschliessend die Signaturen. Nur so erkennt das Tool auch die neuesten Gefahren.

Markieren Sie auf dem Reiter *Scanner* die Option *Vollständigen Suchlauf durchführen* und klicken Sie auf *Scan*. Es öffnet sich ein kleines Fenster, in dem Sie vor jedes zu prüfende Laufwerk ein Häkchen setzen. Mit *Scan starten* beginnen Sie mit der Suche nach Trojanern auf Ihrem Rechner. Bestätigen Sie das Ende des Scans mit einem Klick auf *OK* und klicken Sie anschliessend auf *Ergebnisse anzeigen*.

Schliessen Sie zuerst alle geöffneten Windows-Anwendungen, bevor Sie mit *Entferne Auswahl* die gefundenen Schädlinge in Quarantäne verschieben (siehe unten stehenden Kasten). Es kann sonst zu Problemen bei der Desinfektion kommen.

Auf manchen PCs öffnet sich zunächst ein Fenster *Windows-Dateischutz* mit dem Hinweis, die Windows-CD einzulegen. Das geschieht dann, wenn einer der Schädlinge eine wichtige Systemdatei infiziert und beschädigt hat. Legen Sie in diesem Fall die geforderte CD ein und lassen Sie Windows die Originaldateien wiederherstellen.

Anti-Malware öffnet nach Ende des Scans automatisch den Text-Editor mit einem Protokoll der gefundenen und entfernten Schädlinge. Sie finden diese Datei auch im Ordner *Logs* unterhalb des Installationsverzeichnisses von Anti-Malware.

Eventuell fordert Sie Anti-Malware auf, den PC neu zu starten, um besonders hartnäckige Schädlinge zu entfernen. Klicken Sie in diesem Fall auf *Ja*, um den PC neu zu booten.

Schützen Sie den PC zudem durch einen laufend aktualisierten Virenscanner und spielen Sie immer alle Updates für Windows und installierte Programme ein, um vor Trojanern und anderen Schädlingen geschützt zu sein. *Andreas Th. Fischer*

ANTI-MALWARE 1.32: SO FUNKTIONIERT DAS TOOL

Bevor Anti-Malware 1.32 (kostenlos, www.malwarebytes.org/mbam.php) eine verseuchte Datei oder einen Registry-Schlüssel löscht, verschiebt sie es zuerst in Quarantäne. So verhindert das Tool das versehentliche Löschen wichtiger Daten.

1. **Scanner:** Hier starten Sie einen neuen Scan und löschen gefundene Schädlinge.
2. **Update:** Über diesen Reiter aktualisieren Sie die Signaturen.
3. **Quarantäne:** Hier löschen Sie Schädlinge endgültig von Ihrem PC und stellen desinfizierte Programme wieder her.
4. **Scan-Berichte:** An dieser Stelle sammelt Anti-Malware alle bisherigen Scan-Ergebnisse.
5. **Anbieter:** Die falsch bezeichnete Spalte "Anbieter" listet die Namen der gefundenen Schädlinge auf.
6. **Entferne Auswahl:** Ein Klick auf diesen Button verschiebt die markierten Schädlinge in die Quarantäne.