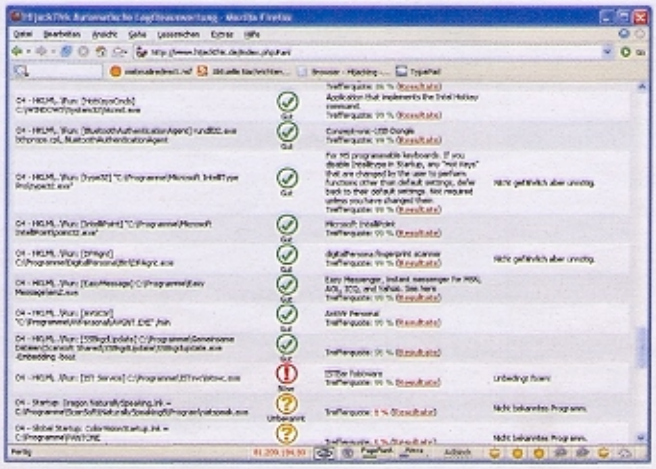


Die Auswertung der Hijack-This-Log-Dateien wird unter www.hijackthis.de entschlüsselt

ware. Daneben sind Tauschbörsen eine wahre Brutstätte für Spionageprogramme. Aber auch vor Internet-Seiten, auf denen »Warez«, also illegale Software, angeboten wird, kann man nur warnen. Meist währt die verbotene Freude über ein geknacktes Programm nur kurz. Denn es liegt nahe, dass kreative Geister mit krimineller Energie, die es schaffen, Programmcode zu knacken, auch vor der Privatsphäre des Benutzers nicht Halt machen. Daneben nutzen Trojaner und Hijacker auch konventionelle Verbreitungstechniken wie E-Mails, freigegebene Laufwerke in LAN und Internet sowie nicht geschlossene Sicherheitslücken in Windows.

Digitaler Selbsterhaltungstrieb

Wie auch normale Programme müssen Hijacker, Viren und Trojaner vom System als ausführbares Programm oder Script geladen werden. Ein Schädling, der nur als Datei auf der Festplatte liegt, kann dem System nichts anhaben. Wird er aber ausgeführt, kann er sein Werk tun. Da der Benutzer den Schädling in der Regel nicht freiwillig startet, nisten sich die Angreifer an all jenen Stellen ein, an denen Windows Programme automatisch startet. Dies sind einerseits der Autostart-Ordner und die NT-Dienste, andererseits aber auch zahlreiche Einträge in der Registrierungsdatenbank. Besonders die Registry wird von aktivierten Hijackern permanent kontrolliert. Entfernt der Benutzer den Registry-Eintrag, fügt ihn der im Hauptspeicher befindliche Eindringling sofort wieder hinzu, um seinen Fortbestand auch nach dem nächsten Systemstart zu gewährleisten. Noch gemeiner ist das Zusammenspiel mehrerer Hijacker, die gleichzeitig im Hauptspeicher sind. Löscht der Anwender den einen Schädling, wird dieser vom anderen Hijacker sofort wieder gestartet.

Grundsäuberung des Systems

Der erste Schritt einer groß angelegten Säuberungsaktion führt über einen Virenscanner und automatische Adware-Vernichter. Sollte Ihr System nicht mit einem aktuellen Scanner geschützt sein, installieren Sie beispielsweise die kostenlose Variante von Antivir (*www.free-av.de*). Zusätzlich hilft die Software Ad-Aware, die ebenfalls kostenlos unter *www.lavasoft.com* zum Download bereitsteht.

Sollte Ihr PC vom Hijacker CWS (Cool Web Search) befallen sein, reichen Ad-Aware und Antivir allerdings nicht aus, um ihn zu eliminieren. Mit dem ebenfalls kostenlosen Tool CWShredder (*www.cwshredder.net*) kann aber auch diesem sehr resistenten Hijacker das Lebenslicht ausgeblasen werden.

Das Problem sämtlicher Tools ist naturgemäß, dass sie nur so aktuell sind, wie ihre Entwickler sie geschaffen haben. So bleiben ganz neue oder rare Hijacker oft außen vor. Hier muss der Benutzer selbst Hand anlegen, um die unerwünschten Programme von seinem Rechner zu entfernen. Dies sollte unbedingt im abgesicherten Modus von Windows geschehen, weil hier nur die nötigsten Systemprogramme geladen werden. Um in diesen Modus zu gelangen,

11 Strategien gegen PC-Schädlinge

Anstatt stundenlang Trojanern, Viren und Hijackern hinterherzurennen, ist es besser, den PC von vorneherein so gut wie möglich abzusichern. Mit folgenden Strategien bleibt Ihr PC von digitalen Schädlingen verschont.

1. Installieren Sie das Windows Service-Pack 2. Das schließt zahlreiche Schlupflöcher des Betriebssystems.

2. Aktivieren Sie die automatischen Update-Funktionen von Windows XP *(Systemsteuerung/Automatische Updates)*. Dadurch werden Bugfixes von Microsoft zeitnah installiert, bevor Eindringlinge die Hintertüren nutzen können.

3. Verwenden Sie eine Firewall. Dadurch werden nur zugelassene Informationen nach außen gegeben. Für den grundlegenden Schutz reicht die Windows-eigene Firewall aus. Mehr Sicherheit bieten beispielsweise Zone Alarm *(www.zonelabs.com)* oder Personal Firewall *(www.sygate.de)*. Beide sind für Privatnutzer kostenlos.

4. Meldet die Firewall, dass ein Programm Daten übers Internet übertragen will, googeln Sie zunächst nach dem Dateinamen, um festzustellen, ob es sich um ein schädliches Programm handelt.

5. Achten Sie bei kostenloser Software darauf, ob diese durch Adware finanziert wird. Eine sehr umfangreiche Liste findet man unter *www.spywareguide.com*.

6. Installieren Sie einen Virenwächter und aktualisieren Sie die Signaturen in regelmäßigen Abständen, mindestens einmal wöchentlich. Für den nicht-kommerziellen Einsatz ist Antivir *(www.free-av.de)* kostenlos.

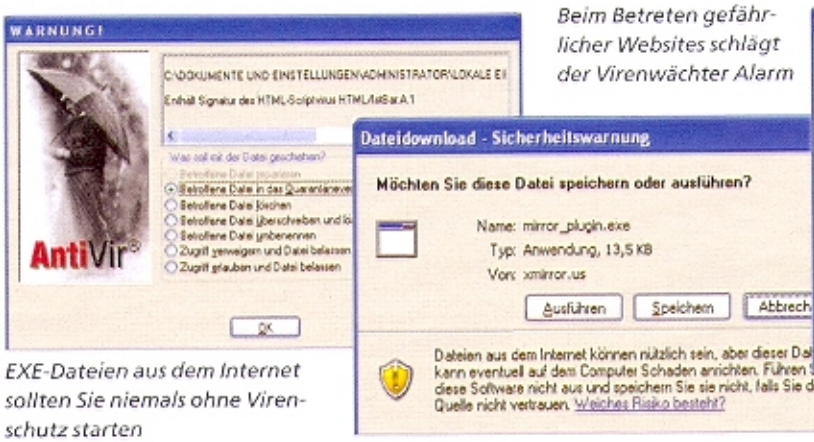
7. Verwenden Sie eine Antispam-Software, wie beispielsweise die Freeware Spamdetacher *(www.fab45.net)*, um E-Mail-Schädlingen noch auf dem Mailserver des Providers den Garaus zu machen.

8. Öffnen Sie niemals E-Mail-Anhänge, wenn Sie den Absender nicht kennen. Auch in Office-Dokumenten können – durch Makroviren übertragen – Trojaner lauern. Achten Sie bei Anhängen auf die Erweiterung. Aktivieren Sie im Explorer die Anzeige der Erweiterungen über *Extras/Ordneroptionen/Ansicht*.

9. Auch wenn die Versuchung groß ist: Nutzen Sie keine illegale Software aus dem Internet. Trotz Virenscanner können neue Trojaner so auf Ihr System gelangen.

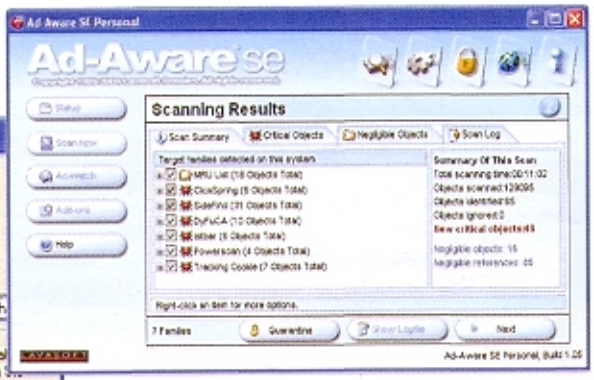
10. Rufen Sie in regelmäßigen Abständen mit [Strg + Alt + Entf] den Task-Manager von Windows auf und schauen Sie sich Systemleistung und Prozesse an. Fallen Ihnen unklare Einträge auf, googeln Sie nach dem Dateinamen.

11. Legen Sie neben dem Standard-User unter Windows XP ein einfaches Benutzerkonto mit eingeschränkten Rechten an. Dadurch beschneidet das System viele Aktivitäten potenzieller Eindringlinge, weil etwa der Zugriff auf Systemdateien oder die Registry verboten oder doch zumindest sehr eingeschränkt ist. Die tatsächlichen Administratorrechte brauchen Sie nur bei der Änderung der Hardware, der Installation von Treibern und Systemtools, aber nicht für die tägliche Arbeit.



Beim Betreten gefährlicher Websites schlägt der Virenwächter Alarm

EXE-Dateien aus dem Internet sollten Sie niemals ohne Virenschutz starten



Die Freeware Ad-Aware findet Werbeeinträge in der Registry ebenso wie Trojaner

drücken Sie beim Start Ihres Rechners mehrfach die Taste [F8], bis das Auswahlmenü erscheint, in dem der abgesicherte Modus aktiviert werden kann.

Die Registry überwachen

Das Überleben von Trojanern und Hijackern hängt davon ab, dass sie bei jedem Start erneut den Weg in den Hauptspeicher finden. Daher überwachen diese Programme ständig die Registrierungsdatenbank von Windows. Mit dem kostenlosen Tool Regmon (*www.sysinternals.com*) können Sie die unerwünschten Registry-Abfragen und -Änderungen kontrollieren.

Nach dem Start von Regmon erscheint eine tabellarische Aufstellung sämtlicher Prozesse, die gerade dabei sind, Registry-Einträge auszulesen oder sie zu verändern. Um nicht im Wust der Einträge zu ertrinken, klicken Sie auf bekannte Prozesse mit der rechten Maustaste und wählen Sie den Eintrag *Exclude process*. Wiederholen Sie dies mit allen Prozessen, die Sie zuordnen können. Fällt Ihnen das schwer, suchen Sie beispielsweise unter *www.liutilities.com/products/wintaskspro/processlibrary*, ob es sich beim jeweiligen Prozess um Spyware handelt. Googeln Sie alternativ nach dem Namen des Prozesses und Sie finden schnell die Information, ob dieser schädlich ist oder nicht. Notieren Sie sich sämtliche unerwünschten Prozesse. Ist die Liste komplett, öffnen Sie mit [Strg + Alt + Entf] den Windows-Task-Manager. Klicken Sie auf das Register *Prozesse* und dann auf den Spaltentitel *Name*, um die Prozesse nach Namen sortiert anzuzeigen. Markieren Sie nun zügig nacheinander die notierten Prozesse und löschen Sie sie mit [Entf]. Warten Sie anschließend eine Weile und sehen Sie nach, ob die Prozesse nachgeladen werden. Ist dies der Fall, haben Sie eine Spyware übersehen, die ihre Kollegen nachlädt.

Den Rechner analysieren

Sind alle schädlichen Prozesse analysiert und mit dem Task-Manager deaktiviert, können Sie mit dem Programm *Hijack This* verhindern, dass diese beim nächsten Systemstart wieder in den Hauptspeicher gelangen.

Laden Sie zunächst von *www.hijackthis.de* das ZIP-Archiv herunter und entpacken Sie es. Das Programm selbst kann ohne Installation gestartet werden. Klicken Sie nach dem Start auf die oberste Schaltfläche. Hijack This analysiert sämtliche Autostart-Bereiche des Systems und listet diese auf. Zusätzlich erzeugt das Programm eine Reportdatei, die auch gleich im Editor geöffnet wird. Markieren Sie den gesamten Editor-Inhalt mit [Strg + A] und kopieren Sie den Text in die Zwischenablage. Öffnen Sie im Browser die Seite *www.hijackthis.de* und fügen Sie im Eingabefeld den Inhalt der Zwischenablage ein. Klicken Sie dann auf die Schaltfläche *Auswerten*. Die ansonsten eher kryptischen Informationen von Hijack This werden nun in lesbare umgesetzt. Interessant sind vor allem sämtliche Einträge, die ein Fragezeichen oder ein rotes Ausrufezeichen aufweisen. Jene rot markierten Elemente sind mit größter Wahrscheinlichkeit Spionageprogramme. Suchen Sie die zugehörigen Einträge innerhalb von Hijack This und markieren Sie sie mit einem Häkchen.

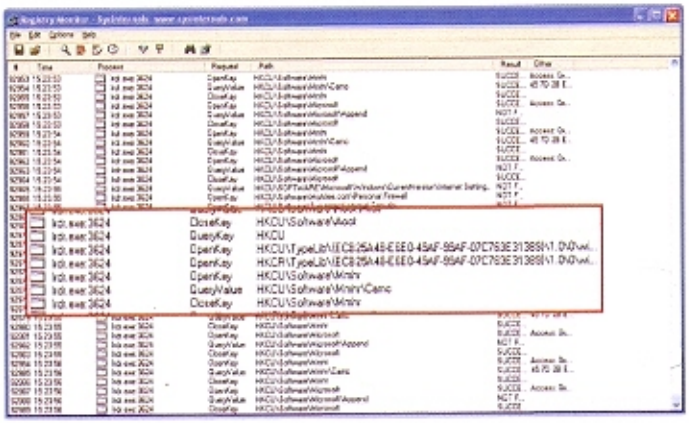
Als Nächstes prüfen Sie sämtliche gelb markierten Einträge, indem Sie wie oben beschrieben Google oder *liutilities.com* befragen, ob es sich um einen Schädling handelt. Sollte das der Fall sein, markieren Sie diesen ebenso in der Hijack-This-Liste. Klicken Sie dann auf *Checked Fixed*, werden sämtliche markierten Verknüpfungen aus den Starteinträgen gelöscht.

Starten Sie anschließend Windows neu und überprüfen Sie, ob Sie den Rechner erfolgreich von den unerwünschten Programmen gesäubert haben.

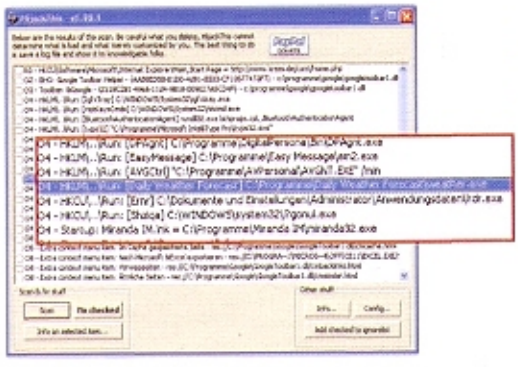
Hinweis: Dem Eindringling Cool Web Search ist mit Hijack This ebenso wenig beizukommen wie mit Antivir und Ad-Aware. Der Schädling weiß, dass Hijack This für ihn und seinesgleichen ein Problem darstellt und hindert das Programm daran, gefixte Einträge auch wirklich zu löschen. Haben Änderungen in Hijack This keine Wirkung, führen Sie also als Erstes den CWShredder aus. *IB*

Weitere Infos

- Netzwerk-Virenscanner
  PC Professionell 04/2005, Seite N6
- Backgroundwissen zu Trojanern
  www.trojaner-info.de
- Deutsches Forum zu Hijack This
  www.hijackthis.de
- Forum für Sicherheitsfragen
  http://board.protecus.de



Der kostenlose Registry Monitor überwacht laufend alle Zugriffe auf die Registrierungsdatenbank, wodurch aktive Trojaner identifiziert werden können



Spyware tarnt sich häufig mit harmlosen Namen, wie hier als weather.exe