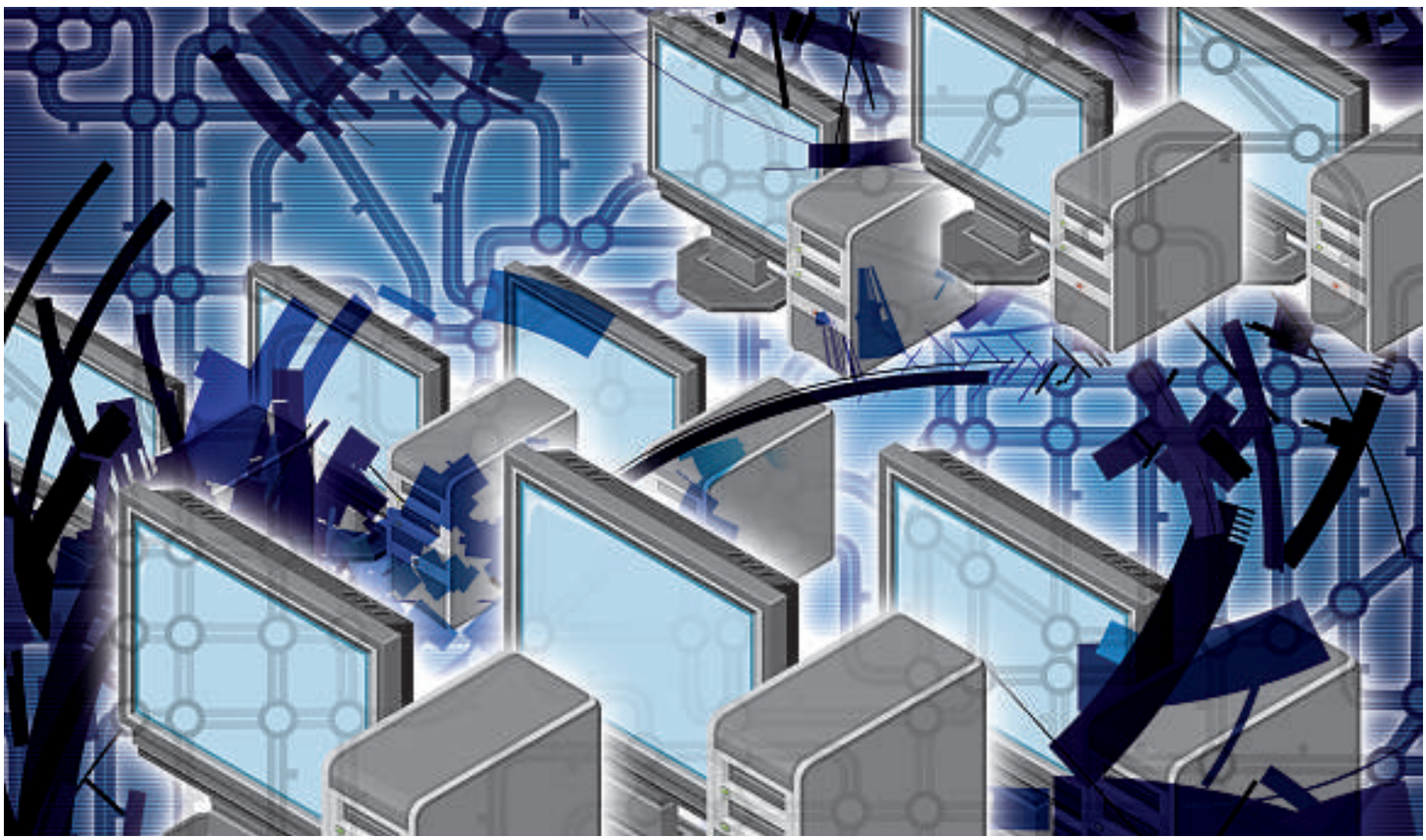


Bot-Viren aufspüren und entfernen

Bot-Viren schleichen sich auf fremden PCs ein, missbrauchen sie für kriminelle Zwecke und schliessen die ferngesteuerten Rechner zu gigantischen Bot-Netzen zusammen. So erkennen Sie Bot-Viren und entfernen sie von Ihrem Computer.

Knapp zwei Millionen PCs umfasst das bislang grösste aufgedeckte Bot-Netz. Das sind zwei Millionen Computer, die bei Privatpersonen, in Firmen oder in Behörden stehen und die heimlich und ohne Kenntnis der Besitzer mit einem Bot-Virus verseucht sind.

Jeder dieser Rechner wird von einem zentralen Steuerungscomputer in der Ukraine kontrolliert, berichtete der Sicherheitsspezialist Finjan, der das Bot-Netz entdeckt hatte (**www.finjan.com/MCRCblog.aspx?EntrId=2237**). Über diesen Rechner haben die Kriminellen vollen Zugriff auf alle verseuchten PCs: Der Bot-Virus kann weiteren Schadcode herunterladen, Bank- und andere Zugangsdaten klauen, Internetserver angreifen, Spam versenden oder für den Benutzer unsichtbar Webseiten aufrufen, um so Werbegeld in die Kassen der Bot-Netz-Betreiber zu spülen.

Kompakt

- *Bot-Viren verwandeln PCs in Zombie-Rechner, die Daten klauen, Spam versenden und Server angreifen.*
- *Hacker schliessen Millionen verseuchter PCs zu Bot-Netzen zusammen und nutzen sie für kriminelle Zwecke.*
- *Der Artikel beschreibt, wie Sie Bot-Viren aufspüren und bekämpfen.*

Ein Bot-Virus unterscheidet sich von einem herkömmlichen Virus: Die kriminellen Banden hinter den Bot-Netzen wollen es unbedingt vermeiden, dass ihre Schädlinge auffallen und bekämpft werden. Selbst ein vermeintlich reibungslos funktionierender und sauberer PC kann mit einem Bot-Virus verseucht sein, aber sich trotzdem äusserlich völlig normal verhalten.

Der Artikel beschreibt, wie Sie solche Bot-Viren und andere Windows-Schädlinge auf Ihrem Computer aufspüren und wie Sie diese Übeltäter bekämpfen. Alle dafür benötigten

Fotos: Mathias Vietmeier

auf DVD

Sicherheitsprogramme finden Sie auf Heft-DVD beziehungsweise kostenlos zum Download im Internet.

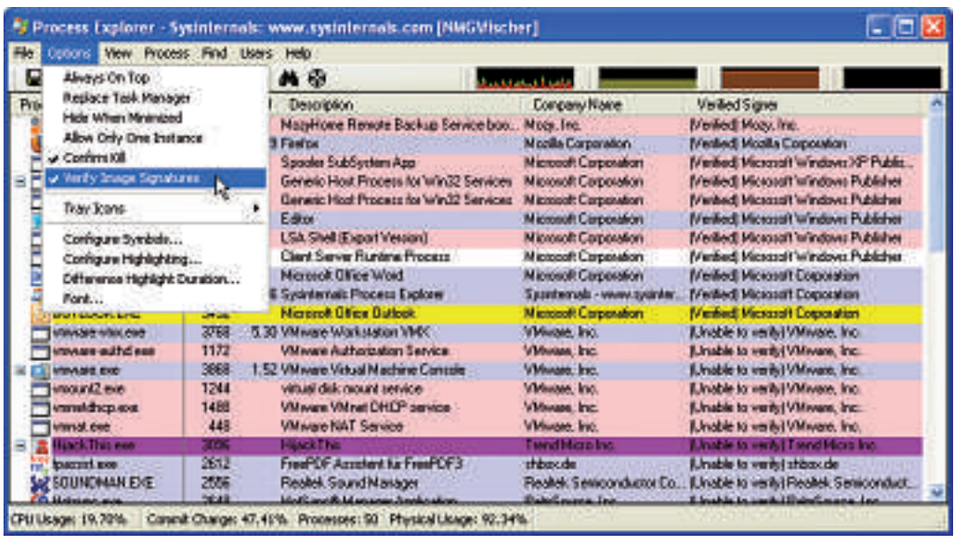
Bot-Infektion aufspüren

Ein moderner Bot-Virus will vor allem eins: nicht auffallen. Während frühere Viren Daten gelöscht und Festplatten formatiert haben, verhält sich ein Bot-Virus völlig unauffällig. Nur so kann er seinen Zweck erfüllen: Daten ausspionieren, Spam versenden und fremde Server im Internet angreifen.

Prozesse untersuchen

Die meisten heimlichen Schädlinge lassen sich über ihre Prozesse aufspüren, mit denen sie unter Windows laufen. Der Task-Manager von Windows bietet jedoch nur wenige Funktionen, um einen Prozess genau zu untersuchen. Weit hilfreicher ist der Process Explorer 11.33 (kostenlos, **http://technet.microsoft.com/de-de/sysinternals/bb896653.aspx** und auf) von Microsoft.

So geht's: Process Explorer muss nicht installiert werden. Entpacken Sie das Archiv und starten Sie das Tool per Doppelklick auf *procexp.exe*. Beim ersten Aufruf bestätigen Sie die Lizenzvereinbarung mit *Agree*. Das Tool zeigt Ihnen sofort alle aktiven Prozesse an.



Process Explorer 11.33: Der Befehl *Options, Verify Image Signatures* prüft die Signaturen aller Prozesse und hilft so, verdächtige Prozesse aufzuspüren (Bild A).

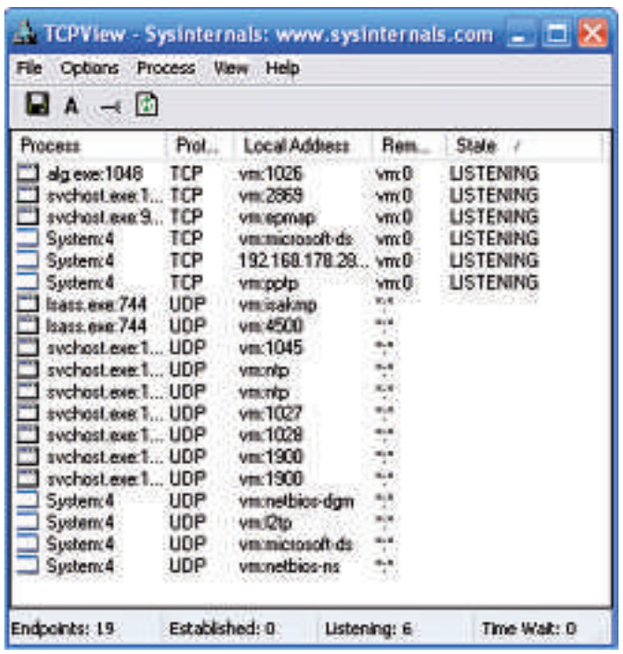
Bringen Sie zuerst Ordnung in die Prozessübersicht: Rufen Sie dazu den Menüpunkt *View, Select Columns…* auf und setzen Sie auf dem Reiter *Process Image* ein Häkchen vor *Verified Signer*. Bestätigen Sie die Änderung mit *OK*. Das Programm blendet jetzt eine zusätzliche Spalte *Verified Signer* ein, in der es anzeigt, ob ein Prozess von Microsoft oder einem anderen Unternehmen geprüft wurde. Ein von einem Schädling veränderter Prozess ▶

verändert seine Signatur und verliert dadurch seinen Verifikationsstatus.

Prüfen Sie nun die Signaturen aller Prozesse mit *Options, Verify Image Signatures* (Bild A). Sobald der Vorgang abgeschlossen ist, klicken Sie oben auf die Spaltenbezeichnung *Verified Signer*. Damit sortieren Sie die Prozesse in verifizierte und nicht verifizierte Prozesse.

Richten Sie besonderes Augenmerk auf alle Prozesse, bei denen in der Spalte *Verified Signer* der Eintrag *Unable to Verify* steht. Klicken Sie mit der rechten Maustaste auf jeden Prozess, der Ihnen unbekannt ist oder verdächtig vorkommt, und wählen Sie *Properties…* aus. Unter *TCP/IP* sehen Sie jetzt alle Internetverbindungen, die der Prozess aufgebaut hat.

Der Reiter *Strings* hilft ebenfalls beim Aufdecken eines Schädlings: Viele Viren versuchen, Virenscanner abzuschiessen. Finden sich unter *Strings* die Namen gängiger Antivirenprogramme, haben Sie einen Schädling aufgespürt.



TCP View 2.54: Alle Programme, die das Tool als *LISTENING* aufführt, lauschen auf Kommunikation von aussen. Die hier gezeigten sind aber alle legitim (Bild B).

Netzwerkverbindungen prüfen

Selbst der geheimste Bot-Virus muss sich doch enttarnen, um Kontakt mit dem Steuerungsserver aufzunehmen. TCP View 2.54 (kostenlos, **http://technet.microsoft.com/de-de/sysinternals/bb897437.aspx** und auf DVD) von Microsoft zeigt offene Netzwerkverbindungen an, auf denen Schädlinge auf Befehle lauschen.

So geht's: TCP View ist wie Process Explorer ein Sofort-Tool und muss nicht installiert werden. Beim ersten Start bestätigen Sie die Lizenzbestimmungen mit einem Klick auf *Agree*. Danach zeigt TCP View sofort alle offenen Netzwerkverbindungen an.

Gefährlich sind Prozesse, die auf Ihrem PC auf Verbindungen warten. Lauschende Prozesse kennzeichnet das Tool in der Spalte *State* mit dem Begriff *LISTENING* (Bild B). Klicken Sie auf *State*, um die Prozesse zu sortieren, und prüfen Sie dann sämtliche *LISTENING*-Einträge. Klicken Sie mit der rechten Maustaste auf dubiose Einträge und wählen Sie *Process Properties…* aus, um sich die Eigenschaften dieses Prozesses anzeigen zu lassen. Sie erfahren dort den ausführlichen Namen des Prozesses sowie den Namen des Unternehmens, das dahintersteht.

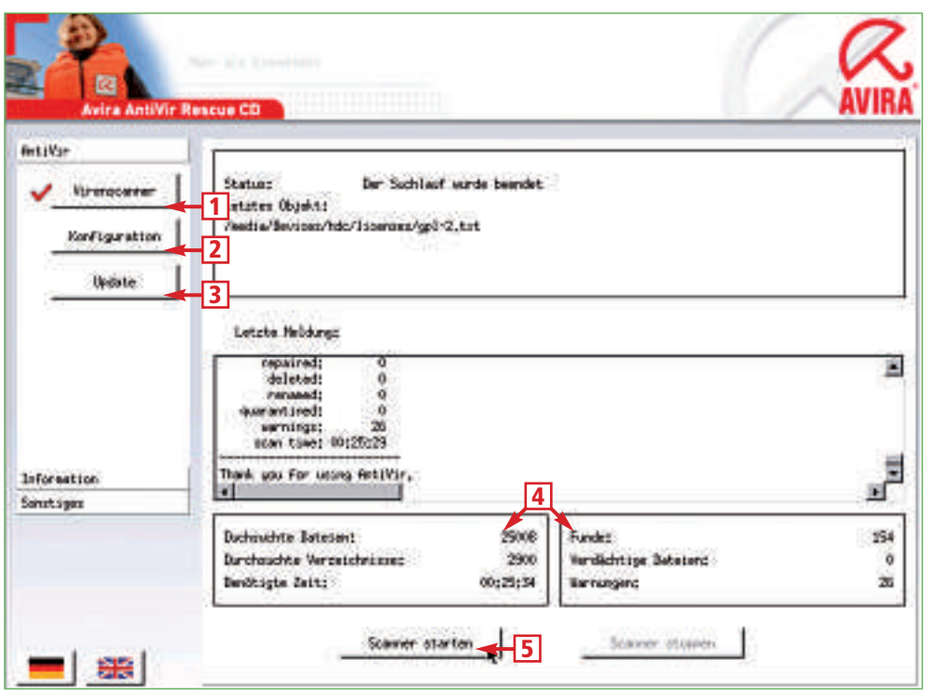
Autostarts ausmisten

Ein Bot-Virus muss sicherstellen, dass er bei jedem Windows-Start geladen wird. Nur so ist er erreichbar, kann Befehle entgegennehmen und seine Aufgaben erfüllen.

Hijack This 2.0.2 (kostenlos, **www.trendsecure.com/portal/de/tools/security_tools/** ▶

Avira Rescue-System 3.6.9: So funktioniert die CD gegen Viren

Das Avira Rescue-System 3.6.9 (kostenlos, www.free-av.de/de/tools/12/avira_antivir_rescue_system.html und auf DVD) brennen Sie auf eine CD, von der Sie dann Ihren PC booten. Danach genügt ein Klick auf *Scanner starten*, um nach Schädlingen zu suchen.



1 Virenscanner
Der Button öffnet den auf dem Bild zu sehenden Dialog. Darin starten Sie eine neue Suche und können Statistiken einsehen.

2 Konfiguration
Hier stellen Sie ein, ob die Live-CD gefundene Viren nur meldet oder ob sie infizierte Dateien repariert beziehungsweise sofort löscht.

3 Update
Wenn Sie einen DSL-Router mit DHCP besitzen, lässt sich hier ein Update der Signaturen starten.

4 Statistiken
Die Live-CD zeigt genau an, wie viele Dateien und Ordner sie gescannt hat und wie viele davon infiziert sind.

5 Scanner starten
Der Button startet die Suche nach Schädlingen auf Ihrem PC.

hijackthis und auf) prüft die Autostart-Bereiche, zeigt alle Elemente an und entfernt gefährliche oder störende Einträge. Das Tool ist auch praktisch, wenn Sie lästige Autostart-Einträge entfernen wollen, wie sie etwa Quicktime anlegt.

So geht's: Starten Sie die Installation von Hijack This mit einem Doppelklick auf *HJTInstall.exe*. Nach dem Setup öffnet sich Hijack This automatisch. Klicken Sie auf *Do a system scan and save a logfile* (Bild C).

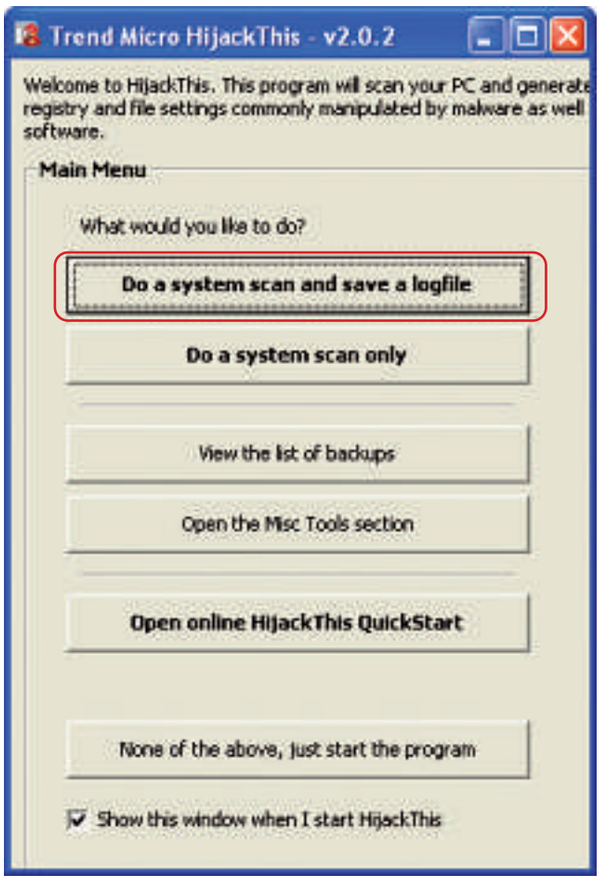
Das Programm prüft nun alle Autostart-Bereiche Ihres PCs und zeigt die Ergebnisse einmal im eigenen Fenster und einmal als Textdatei *hijackthis.log* im Texteditor an. Klicken Sie zuerst in das Fenster des Texteditors und drücken Sie *[Strg A]*, um den gesamten Text zu markieren. Mit *[Strg C]* kopieren Sie ihn in die Zwischenablage.

Öffnen Sie nun ein Browserfenster und rufen Sie die Webseite **www.hijackthis.de** auf. Klicken Sie in das Feld *Kopieren Sie ein Logfile in die Textbox* und drücken Sie *[Strg V]*, um den Inhalt aus Ihrer Zwischenablage einzufügen. Klicken Sie danach auf *Auswerten*, um mit der Überprüfung zu beginnen. Die Webseite vergleicht jeden auf Ihrem PC gefundenen Eintrag mit einer umfangreichen Datenbank. So profitieren Sie von den Erfahrungen anderer Nutzer von Hijack This und finden schnell gefährliche Einträge.

Software-Übersicht

Programm	Quelle	Seite
Adblock Plus 1.0.2 (Werbeblocker)	http://adblockplus.org/de	47
Avira Rescue-System 3.6.9 (Antiviren-Live-CD)	www.free-av.de/de/tools/12/avira_antivir_rescue_system.html	45
Avast 4.8 (Virenscanner)	www.avast.com	44
Firefox 3.0.10 (Browser)	www.mozilla-europe.org/firefox	47
Hijack This 2.0.2 (Autostart-Tool)	www.trendsecure.com/portal/de/tools/security_tools/hijackthis	42
Mozbackup 1.4.9 (Thunderbird-Backup-Erweiterung)	http://mozbackup.jasnapaka.com/de	47
Noscript 1.9.3.3 (Javascript-Blocker)	www.noscript.net	47
Online Armor Free 3.5.0.14 (Desktop-Firewall)	www.tallemu.de/software/free	47
Process Explorer 11.33 (Prozess-Tool)	http://technet.microsoft.com/de-de/sysinternals/bb896653.aspx	41
Secunia Personal Software Inspector 1.0.0.4 (Update-Tool)	www.secunia.com/vulnerability_scanning/personal	46
Sophos Anti-Rootkit 1.3.1 (Anti-Rootkit-Tool)	www.sophos.de/products/free-tools/sophos-anti-rootkit.html	45
TCP View 2.54 (Netzwerk-Tool)	http://technet.microsoft.com/de-de/sysinternals/bb897437.aspx	42
Thunderbird 2.0.0.21 (Mail-Programm)	www.mozilla-europe.org/thunderbird	47

Alle -Programme finden Sie auf Heft-DVD in der Rubrik *Computer, Bot-Viren.*



Hijack This 2.0.2: Ein Klick auf den rot markierten Button startet die Suche nach verdächtigen Autostart-Einträgen auf Ihrem PC (Bild C).

Wenig später sehen Sie eine Auswertung der Autostart-Elemente auf Ihrem PC. Mit grünen Häkchen versehene Einträge sind unbedenklich. Prüfen Sie jedoch sorgfältig alle mit gelben Fragezeichen und rote Kreuzen markierten Einträge. Sie kennzeichnen verdächtige Elemente, die auf verborgene Schädlinge hinweisen. Per Klick auf die Kästchen in der Spalte *Benutzerbewertung* gelangen Sie zu den Kommentaren anderer Benutzer. Weitere Hinweise erhalten Sie, wenn Sie den Dateinamen und eventuell den angegebenen Windows-Pfad in der Spalte *Meldung* bei einer Suchmaschine eintippen und die Ergebnisse auf Meldungen über Schädlinge überprüfen.

Merken Sie sich anschliessend alle schädlichen Autostart-Einträge, die Sie von Ihrem Computer entfernen wollen, und wechseln Sie wieder zum Programmfenster von Hijack This. Setzen Sie hier je ein Häkchen vor jedes zu entfernende Element und klicken Sie auf *Fix checked*. Aber Vorsicht: Wenn Sie den falschen Eintrag markieren, startet Windows anschliessend eventuell nicht mehr.

Achtung: Hijack This entfernt keine Schädlinge von Ihrem PC, es verhindert nur, dass der Übeltäter sich bei jedem Windows-Start neu aktiviert.

Bot-Infektion bekämpfen

Die wichtigste Massnahme zum Schutz vor Bot-Viren ist die Installation eines Virenscanners, der das Eindringen des Schädlings verhindert. Rootkits bekämpft man dagegen mit einem speziellen Anti-Rootkit-Tool.

Virenscanner

Ein aktueller Virenscanner ist auf jedem Windows-PC zum Schutz gegen Bot-Viren und andere Schädlinge unverzichtbar. Falls Sie noch nicht über ein geeignetes Antivirenprogramm verfügen, empfiehlt sich Avast 4.8 (kostenlos, **www.avast.com** und auf). Einen Test kostenpflichtiger Sicherheits-Suiten finden Sie in Online PC 12/2008 ab Seite 4 (**www.onlinepc.ch/archiv**).

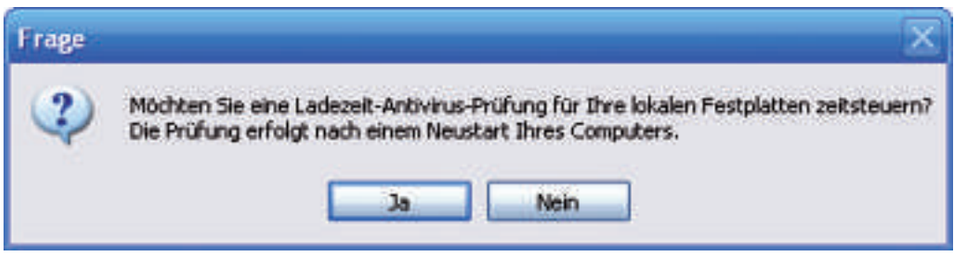
Achtung: Gegen neue Schädlinge, für die es noch keine Signatur gibt, hilft nur verhaltensbasierte Erkennung. Und die bieten ausschliesslich Kaufprogramme.

So geht's: Installieren Sie Avast und klicken Sie bei der Frage nach einer *Ladezeit-Antivirus-Prüfung* auf *Ja* (Bild D). Das Programm prüft Ihren Computer dann beim nächsten Start, noch bevor Windows geladen wurde, auf Schädlinge.

Nach dem Neustart öffnet sich das Willkommensfenster von Avast. Klicken Sie auf den oberen Link und füllen Sie anschliessend im Browser das Registrierungsformular aus. Sie

erhalten nach kurzer Zeit eine E-Mail mit einem kostenlosen Registrierungsschlüssel für 14 Monate, den Sie als Privatanwender beliebig oft erneuern dürfen. Markieren Sie den Registrierungsschlüssel mit der Maus und drücken Sie *[Strg C]*.

Schliessen Sie jetzt das Willkommensfenster mit *OK*. Klicken Sie danach mit der rechten Maustaste auf das Avast-Icon unten rechts im System-Tray und wählen Sie *Über avast!…*, *Lizenz-Schlüssel* aus. Fügen Sie den Schlüssel mit *[Strg V]* ein und bestätigen Sie zwei Mal mit *OK*.



Installation von Avast 4.8: Hier sehen Sie eine schlecht übersetzte Meldung beim Setup von Avast. Damit meint das Tool, ob Sie einen gründlichen Virencheck beim nächsten Boot-Vorgang wünschen (Bild D).

Tool gegen Rootkits

Bot-Viren enthalten heute oft Rootkit-Komponenten. Ein Rootkit manipuliert wichtige Systemtreiber und den Windows-Kernel, um sich so vor Virenscannern und im Windows-Explorer unsichtbar zu machen. Nur Spezial-Tools spüren Rootkits auf und entfernen diese.

So geht's: Installieren Sie Sophos Anti-Rootkit 1.3.1 (kostenlos, **www.sophos.de/products/free-tools/sophos-anti-rootkit.html** und auf) und klicken Sie auf *Ja*, um das Sicherheits-Tool direkt anschliessend zu starten.

Mit *Start scan* beginnen Sie mit der Suche nach aktiven Rootkits auf Ihrem PC. Das Tool prüft die laufenden Prozesse und sucht in der Windows-Registry nach Hinweisen auf die heimlichen Schädlinge (Bild E).

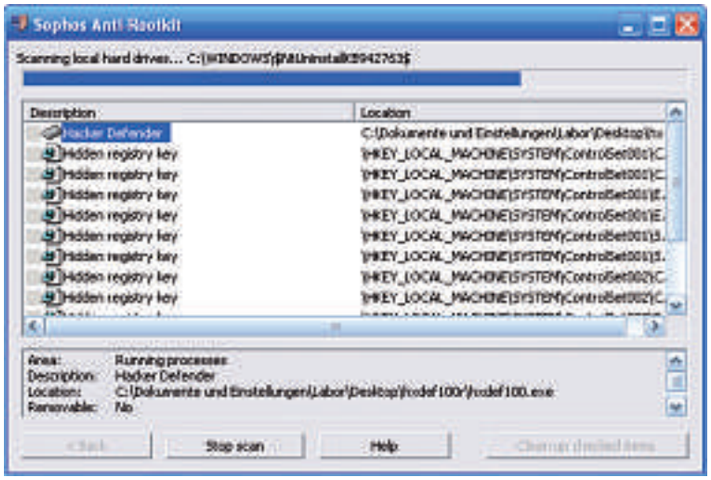
Virenscanner auf CD

Wenn Sie Ihren Computer mit einer bootfähigen Sicherheits-CD prüfen, können sich eventuell vorhandene Schädlinge nicht aktivieren und so auch nicht vor dem Zugriff durch einen Virenscanner schützen. Ein Check per Live-CD ist deswegen in jedem Fall wirksamer als der Scan mit einem unter Windows installierten Virenscanner.

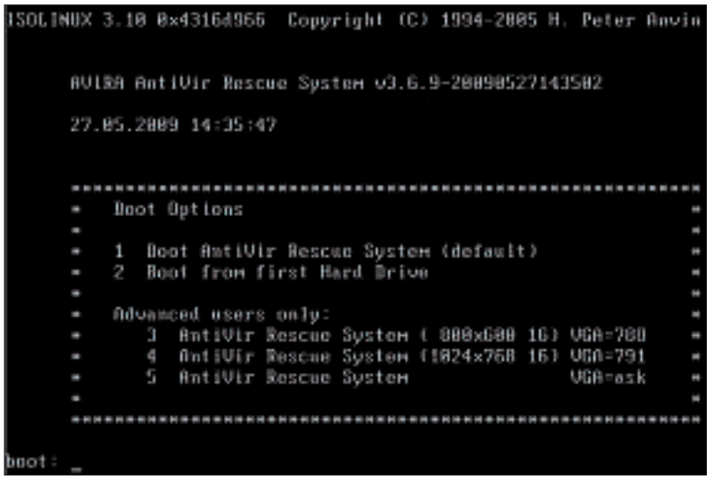
So geht's: Das Rescue-System 3.6.9 von Avira (kostenlos, **www.free-av.de/de/tools/12/avira_antivir_rescue_system.html** und auf) ist eine Linux-Live-CD mit einem integrierten Virenscanner. Die aktuelle Version enthält auch eine Update-Routine für neue Virensignaturen.

Praktischerweise bietet die EXE-Datei des Rescue-Systems bereits ein eigenes Brennmodul, das sich direkt nach dem Start öffnet. Klicken Sie statt auf *Brenne CD* auf *Beenden*, wenn Sie lieber die ISO-Datei extrahieren und mit Ihrem gewohnten Brennprogramm brennen wollen.

Legen Sie die CD nach dem Brennen in das CD/DVD-Laufwerk und booten Sie Ihren PC. Eventuell müssen Sie die Boot-Einstellungen im BIOS Ihres PCs ändern, wenn der Rechner nicht von der CD booten will. Sie öffnen die ▶



Sophos Anti-Rootkit 1.3.1: Der Rootkit-Jäger hat viele versteckte Einträge (*Hidden registry key*) in der Registry gefunden. Das kann auf ein Rootkit hinweisen (Bild E).



Rescue-System 3.6.9: Betätigen Sie an dieser Stelle die Eingabetaste, um Ihren PC von der Antiviren-CD zu starten (Bild F).

BIOS-Einstellungen Ihres Rechners, indem Sie direkt nach dem Einschalten des Computers mehrmals die Taste *[Entf]*, *[F1]* oder *[F2]* drücken. Welches die richtige Taste ist, hängt von Ihrem System ab.

Betätigen Sie die Eingabetaste, sobald die erste Boot-Meldung des Rescue-Systems erscheint (Bild F). Das Antiviren-System startet nun. Sobald die Oberfläche fertig geladen ist, genügt ein Klick auf *Scanner starten*, um mit der Überprüfung des Computers zu beginnen.

Rechts unten sehen Sie eine Übersicht über gefundene Schädlinge. In der Standardeinstellung protokolliert das Rescue-System gefundene Schädlinge nur und entfernt sie nicht. Klicken Sie auf *Konfiguration* und wählen Sie *Versuchen, infizierte Dateien zu reparieren* aus, um Datenverlust zu vermeiden. Wenn Sie *Infizierte Dateien löschen* auswählen, werden möglicherweise wichtige Dateien unwiederbringlich vernichtet. Nutzen Sie diese Option deshalb nur in Ausnahmefällen.

Bot-Infektion verhindern

Mit wenigen Mitteln lässt sich jeder PC so einrichten, dass er sicher vor Bot-Viren ist. Wichtig sind alle Sicherheits-Patches für Windows, das Aktualisieren wichtiger Anwendungen, ein Schutz des Netzwerks und die Wahl sicherer Programme zum Surfen.

Windows aktualisieren

Viele Schädlinge nutzen Windows-Lücken, um sich auf PCs einzuschleichen. Aktuelles Beispiel ist der Wurm Conficker, der eine eigentlich bereits im vergangenen Herbst von Microsoft geschlossene Sicherheitslücke nutzt, um sich zu verbreiten. Das Problem ist, dass viele Windows-Nutzer ihr System nie oder viel zu selten aktualisieren. Aber selbst Nutzer von Raubkopien erhalten von Microsoft alle Sicherheits-Patches und müssen beim Herunterladen keine Probleme befürchten.

So geht's: Rufen Sie *Start, Systemsteuerung, Sicherheitscenter* auf und klicken Sie auf *Automatische Updates*. Wählen Sie *Updates herunterladen, aber Installationszeitpunkt manuell festlegen* aus (Bild G). So erhalten Sie alle Updates schnellstmöglich, verlieren aber nicht die Kontrolle darüber, welche Patches installiert werden. Wann immer ein neues Update bereitsteht, weist Windows Sie unten rechts mit einem gelben Warnzeichen darauf hin.

Windows Update: Die markierte Option bewirkt, dass Sie die Kontrolle über die Patches behalten (Bild G).

Anwendungen aktualisieren

Veraltete Software stellt ein hohes Sicherheitsrisiko dar. Oft findet ein Virus auch noch Monate oder gar Jahre nach Erscheinen eines Sicherheits-Patches noch zahlreiche ungepatchte Systeme. Achten Sie deswegen darauf, die Anwendungen auf Ihrem PC stets aktuell zu halten. Am besten erledigen Sie diese Aufgabe mit dem Secunia Personal Software Inspector 1.0.0.4 (kostenlos, **www.secunia.com/vulnerability_scanning/personal** und auf).

So geht's: Installieren Sie das Tool und starten Sie es mit einem Klick auf *Ja*. Das Programm beginnt sofort damit, nach veralteter Software zu suchen. Anschliessend zeigt es Ihnen die gefundenen Probleme in einer kurzen Statistik an (Bild H).

Klicken Sie danach oben rechts auf *ERWEITERT* und auf *OK*, um die ausführliche Ansicht zu aktivieren. Auf dem Reiter *Unsicher* finden Sie alle veralteten Programme, bei denen Sicherheitslücken bekannt sind. Diese Anwendungen sollten Sie so schnell wie möglich aktualisieren.

Dazu klicken Sie rechts neben dem Programmnamen auf den blauen Button mit dem weissen Pfeil. Das Tool führt Sie auf eine Download-Seite oder teils auch direkt zum Download der aktuellen Version. Gelegentlich sind jedoch englische Programmversionen statt der deutschsprachigen verlinkt. Eine kurze Internetrecherche mit Google führt Sie aber meist schnell zur deutschen Version.

Netzwerk sichern

Eine Firewall verhindert Angriffe aus dem Internet. Sie blockiert Würmer, die Schadsoftware auf dem PC installieren wollen, und kann die Kommunikation eines Bot-Virus mit seinem Steuerserver verhindern.

So geht's: Praktisch alle aktuellen DSL-Router enthalten bereits eine Firewall, die vor Angriffen von aussen schützt. Einen Schutz im internen Netz bieten zudem die integrierten Firewalls von Windows XP ab Service Pack 2 und von Vista.

Nur wer noch seinen PC mit einem Modem direkt mit dem Internet verbindet, sollte unbedingt eine eigene Desktop-Firewall installieren. Eine leistungsfähige, noch relativ unbekannte kostenlose Firewall mit einem besonders ausführlichen Einrichtungsassistenten (Bild I) ist Online Armor Free 3.5.0.14 (kostenlos, **www.tallemu.de/software/free** und auf).

Surfschutz

Der Browser ist eines der wichtigsten Einfallstore für Schädlinge, die sich bereits beim vermeintlich harmlosen Surfen im Internet auf einen fremden PC einschleichen können. Die dabei von den Angreifern verwendete Technik wird Drive-by-Downloads genannt. Es erfolgt also ein Download einer schädlichen Datei "beim Vorbeifahren".

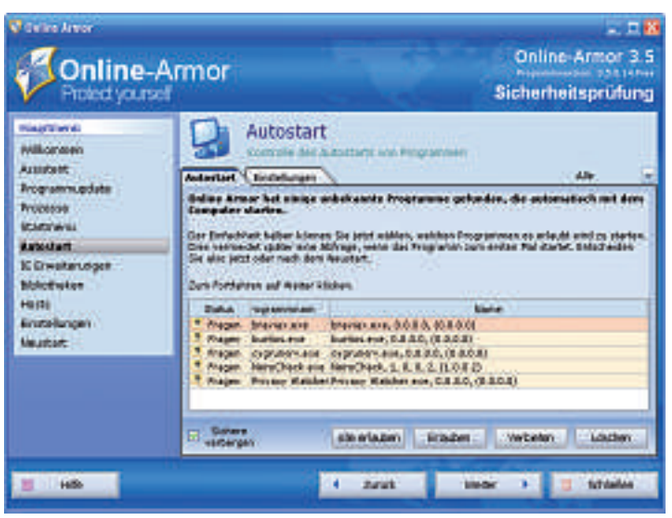
So geht's: Den besten Schutz bietet der Browser Firefox 3.0.10 (kostenlos, **www.mozilla-europe.org/firefox** und auf), weil er laufend aktualisiert und verbessert wird und weil er sich mit kostenlosen Erweiterungen weiter sichern lässt.

Bewährt haben sich der Javascript-Blocker Noscript 1.9.3.3 (kostenlos, **www.noscript.net** und auf) und der Werbeblocker Adblock Plus 1.0.2 (kostenlos, **http://adblockplus.org/de** und auf). Das Blockieren von Javascript und das Sperren der Internetwerbung ist deswegen so wichtig, weil die Internetkriminellen immer wieder manipulierte Banner in grosse Werbenetze eingeschleust haben.

Eine Infektion kann dann auch beim Besuch einer eigentlich seriösen Seite erfolgen: Das manipulierte Banner nutzt dabei oft eine Sicherheitslücke in Adobe Flash aus und platziert einen Dropper auf dem Computer, der dann erst den eigentlichen Schädling herunterlädt und aktiviert.

Der Javascript- und der Werbeblocker lassen sich bei Bedarf ausschalten.

Secunia Personal Software Inspector 1.0.0.4: Die gefährlichsten Bedrohungen durch veraltete Software auf Ihrem PC zeigt das Tool in einer Übersicht an (Bild H).



Online Armor Free 3.5.0.14: Der Assistent zeigt eventuell riskante Autostart-Einträge an. Auf dem Screenshot ist nur *NeroCheck.exe* von einem seriösen Anbieter, der Rest stammt von Schädlingen (Bild I).

Mailschutz

Die Zahl infizierter Spam-Mails hat zwar nachgelassen, es versuchen aber immer noch einige Schädlinge, sich über Mails zu verbreiten. Der grösste Teil davon sind Trojaner und Würmer, die selbstständig Spam versenden, ohne dass der Besitzer es bemerkt. Dabei nutzen sie immer wieder Lücken in den verbreiteten Mail-Programmen Outlook und Windows Mail aus. Mehr Sicherheit beim Mailen bietet Thunderbird 2.0.0.21 (kostenlos, **www.mozilla-europe.org/thunderbird** und auf).

So geht's: Installieren und starten Sie Thunderbird. Beim ersten Aufruf öffnet sich automatisch ein Assistent, der Ihnen beim Einrichten Ihres Mail-Kontos hilft. Falls Sie Thunderbird als Standardprogramm für Mails verwenden wollen, ist Mozbackup 1.4.9 (kostenlos, **http://mozbackup.jasnapaka.com/de** und auf) ein nützliches Tool, das Ihre Einstellungen und Mails sichert. Bestimmen Sie den Ort, an dem Sie die Sicherungskopien speichern wollen, und geben Sie an, ob die Kopien verschlüsselt werden sollen. ■

Andreas Th. Fischer