

ARTIKEL-
WEGWEISER

- Die fünf übelsten Betrüger-Programme Seite 47
- Betrüger-Programme loswerden Seite 48
- Diese 122 Programme erpressen und betrügen Seite 52
- So testet COMPUTERBILD Seite 54

(M) Foto: RTL II, Montage: COMPUTERBILD



Nützlicher Helfer oder fieser Spion? Mit dieser Frage hat „24“-Agent Jack Bauer mächtig Stress, Sie wissen's nach ein paar Mausklicks: COMPUTERBILD hilft Ihnen bei der Jagd nach Betrüger-Software in Ihrem PC.

Du willst doch nicht, dass Deine Pizzeria abbrennt, oder? Dann musst Du zahlen, und wir beschützen Dich!“ Diese klassische Mafia-Methode haben Softwarebetrüger verfeinert: Mit miesen Tricks verkaufen sie für viel Geld wirkungslose Sicherheitssoftware. Tausende PC-Nutzer sind schon zu Opfern gewor-

den, und viele haben's noch nicht mal bemerkt. Denn die Programme geben vor, den Computer zu schützen. Doch das ist nur Show: In Wirklichkeit haben Schädlinge leichtes Spiel, weil keins der Programme sie ernsthaft bekämpft. Dadurch sind Ihre Daten in großer Gefahr. COMPUTERBILD deckt die üble Masche auf und nennt 122 Programme, die lügen, erpressen und betrügen.

Habe ich so ein Programm auf meinem PC?

Das müssen Sie mit der Anleitung von COMPUTERBILD so schnell wie möglich überprüfen. Zunächst stellen Sie fest, welche Programme auf Ihrem PC vorhanden sind. Wie das geht, steht auf Seite 48. Die Einträge in der Programmliste vergleichen

Sie dann mit der Tabelle auf Seite 52. Dort sind alle 122 gefährlichen Programme aufgelistet. Gibt es Übereinstimmungen? Dann müssen Sie sofort handeln.

Wie entferne ich die Betrüger-Software?

Einigen Betrüger-Programmen macht seriöse Antiviren-Software wie die Kaspersky Security Suite (auf Heft-CD/-DVD) den Garaus. Trotzdem bleiben Lücken, denn Antiviren-Programme können gezielt nach Schädlingen suchen, aber nicht jeden Betrug erkennen. COMPUTERBILD erklärt, wie Sie die Plagegeister entfernen:

Das können Betrüger-Programme anrichten:

■ Abzocke mit Gratis-Versionen:

Nur die Prüfung auf Gefahren ist kostenlos, für die Abwehr wird zur Kasse gebeten!

■ Erpressung mit Falschmeldungen:

Schädlinge werden einfach erfunden. So werden Sie zum Kauf der Vollversion erpresst.

■ Vorsätzliche Virenverseuchung:

Einige Programme bringen Viren mit, um ihre angeblichen Fähigkeiten zu demonstrieren.

■ Windows wird zerstört:

Sogar wichtige Windows-Dateien werden gelöscht. Das Ergebnis: Nichts geht mehr.

■ Extreme Viren-Gefahr:

Der Nutzer glaubt, er sei sicher. Doch das Programm ist wirkungslos, der PC gefährdet.

■ Manipulation am Internet-Zugriffsprogramm:

Änderungen am Zugriffsprogramm gefährden die Sicherheit. Ein Riesens-Einfallstor für Viren.

■ **Schritt 1:** Zunächst versuchen Sie, das Betrüger-Programm auf normalem Windows-Weg über das Menü „Software“ zu entfernen (Seite 48).



Mafia-Methode: Erst erfinden Betrüger einen Schädling, dann lassen sie sich seine Entfernung auch noch bezahlen.

■ **Schritt 2:** Da viele Betrügerprogramme auch nach der Deinstallation noch gefährliche Reste auf dem PC hinterlassen, müssen Sie den Computer anschließend mit der Antispyware-Software „A-Squared“ von der Heft-CD/DVD überprüfen. Das Programm schaltet die Betrüger endgültig ab. Keine Angst: Sie können A-Squared ohne Probleme zu-

sätzlich zu einem Antiviren-Programm verwenden (Seite 48).

■ **Schritt 3:** Zuletzt beseitigen Sie noch die letzten möglichen Spuren der Betrüger. Dazu verwenden Sie das Programm „CCleaner“ von der Heft-CD/DVD. Der sieht sich die Registrierungs-Datenbank (S.56) **01** genau an und entfernt Überbleibsel (Seite 50).

Keins meiner Programme steht in der Liste. Bin ich dann sicher?

Dafür gibt's leider keine Garantie. Denn die Software-Mafia reagiert schnell auf eine Enttarnung, um den Geldfluss nicht versiegen zu lassen. Die Betrüger ändern einfach die Programmnamen und die Oberfläche der Software. Deswegen: Auch

wenn Sie bisher verschont geblieben sind, sollten Sie Ihren Computer mit A-Squared und CCleaner überprüfen. Denn vielleicht treibt auf Ihrem PC schon ein neues Betrüger-Programm sein Unwesen. Und: Machen Sie beim Thema Sicherheit keine Experimente. Vertrauen Sie nur auf Programme, die COMPUTERBILD getestet hat.

Die fünf übelsten Betrüger-Programme

Hier zeigt COMPUTERBILD anhand von fünf Programmen, wie die Software-Mafia vorgeht. Aggressive Wer-

bung für nutzlose Vollversionen, übertriebene Gefahrenmeldungen und Erpressung durch erfundene

Schädlinge gehören zum Standard. Wer die Tricks einmal durchschaut hat, fällt künftig nicht mehr auf die

Masche rein. Eine Liste mit bisher entdeckten Betrüger-Programmen finden Sie ab Seite 52.

1 Spyware Soft Stop



Spyware Soft Stop ist besonders dreist: Die „Vorhut“ versteckt sich in kostenlosen Programmen aus dem Internet und wird unbemerkt mitinstalliert. Künftig nerven aufklappende Fenster **1**, die zum Teil sogar aussehen wie das Windows-Update **2**. Sie verleiten zum Überspielen der Vollversion. Wer darauf reinfällt und auf „Yes“ klickt, installiert die Betrüger-Software und außerdem diverse Schadprogramme. Und die lassen sich nur nach Bezahlung von 45 Euro vom PC entfernen. Glatte Erpressung!

2 One-Shot Antivirus



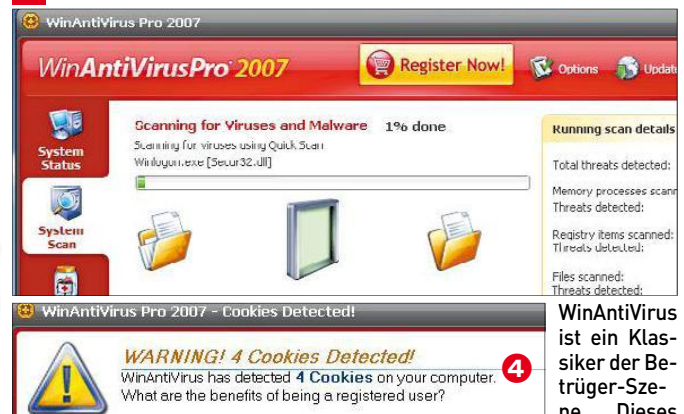
Vor diesem Programm müssen Sie besonders vorsichtig sein. „One-Shot Antivirus“ ist selbst ein Virus und macht die Arbeit mit dem Computer beinahe unmöglich. Alle drei Stunden schaltet sich der PC ab und startet neu, viele Windows-Funktionen sind nicht mehr nutzbar.

3 Spyware Secure



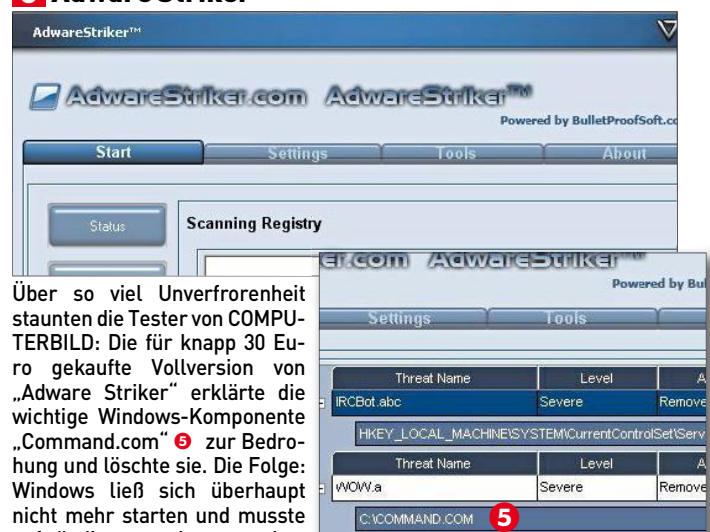
„Spyware Secure“ findet Schädlinge, die gar nicht da sind und macht aggressive Werbung. Alle paar Minuten tauchen Hinweissfenster auf und warnen vor angeblicher Bedrohung **3**. Einziges Ziel: Das Opfer soll die Vollversion für rund 40 Euro kaufen.

4 WinAntiVirus



WinAntiVirus ist ein Klassiker der Betrüger-Szene. Dieses Programm erscheint in immer neuen Versionen. Die Urheber sitzen vermutlich in der Ukraine und verkaufen ihr angebliches Antiviren-Programm inzwischen sogar als komplettes Internet-Schutzpaket für 69 Euro. Die Testversionen können nichts gegen Viren ausrichten, nerven mit völlig überzogenen Warnmeldungen **4** und Hinweisen auf die Kaufversion. Doch selbst die kostenpflichtige Vollversion ist absolut untauglich, um den PC effektiv vor Schädlingen zu schützen. Sie entdeckte von mehreren Zehntausend Viren nur wenige Dutzend.

5 Adware Striker



Über so viel Unverfrorenheit staunten die Tester von COMPUTERBILD: Die für knapp 30 Euro gekaufte Vollversion von „Adware Striker“ erklärte die wichtige Windows-Komponente „Command.com“ **5** zur Bedrohung und löschte sie. Die Folge: Windows ließ sich überhaupt nicht mehr starten und musste aufwändig repariert werden. Nur ein Beispiel dafür, wie schnell solche Programme das gesamte Computersystem lahmlegen können. Hersteller „Bulletproofsoft“ ist kein Unbekannter in der Szene. Wie bei vielen anderen Urhebern solcher Software ist unklar, wer wirklich dahinter steckt. Die Internetadresse wurde anonym registriert, auf Anfragen gibt es keine Antwort.

Gefährliche Programme loswerden

Haben Sie in der Tabelle auf Seite 52 ein Programm entdeckt, dass auch auf Ihrem PC installiert ist? Dann sollten Sie es schnellstens entfernen. Denn ein wirkungsloses

Schutzprogramm hilft Ihnen nicht. Außerdem bringen manche dieser angeblichen Antispyware-Programme sogar noch Schädlinge mit. Leider hilft das Deinstallieren über das

„Software“-Menü von Windows nicht immer weiter. Denn die Programme verstecken wichtige Bestandteile und halten sich hartnäckig auf der Festplatte und in der

Registrierungs-Datenbank (S.56) [01]. Mit den Programmen „A-Squared“ und „CCleaner“ von der Heft-CD/-DVD finden und entfernen Sie solche gefährlichen Überbleibsel.

Schritt 1: Programme identifizieren und deinstallieren

Befindet sich ein Schummel-Programm auf Ihrer Festplatte? Mit der folgenden Anleitung finden Sie es heraus. Außerdem erfahren Sie, wie Sie die Software im Fall der Fälle wieder loswerden:

1 Starten Sie die Systemsteuerung von Windows. Dazu klicken Sie zunächst auf die Schaltflächen **Start** und **Systemsteuerung** und anschließend auf **Software**. Im nächsten Fenster erscheint eine Liste installierter Programme, in diesem Beispiel:

2 Vergleichen Sie die Liste mit der Tabelle ab Seite 52. Ist keins der aufgeführten Programme in Ihrer Liste? Dann machen Sie gleich

mit dem nächsten Abschnitt „Versteckte Programme und Schädlinge mit „A-Squared“ entfernen“ weiter. Andernfalls klicken Sie auf den Bö-



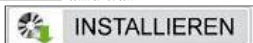
sewicht, im Beispiel auf **SpywareSoftStop**, damit der Eintrag blau hinterlegt erscheint. Es folgt ein Mausklick auf **Entfernen** oder auf **Ändern/Entfernen**.

3 Folgen Sie den weiteren Anweisungen auf dem Bildschirm, um das Programm zu deinstallieren. Im Beispiel klicken Sie dazu auf **Ja** und dann auf **OK**. Wiederholen Sie dies gegebenenfalls mit weiteren Programmen aus der Tabelle. Nach einem Neustart von Windows machen Sie dann mit dem nächsten Abschnitt weiter.

Schritt 2: Versteckte Programme und Schädlinge mit „A-Squared“ entfernen

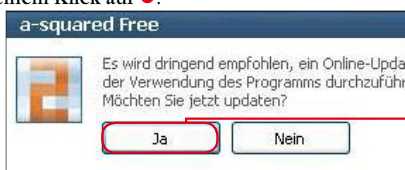
Trotz Deinstallation bleiben fast immer Reste einer Schummel-Software auf der Festplatte zurück. Häufig handelt es sich dabei um harmlose Überbleibsel, in manchen Fällen aber auch um gefährliche Schadsoftware (siehe Tabelle auf Seite 52). Um diese Reste und versteckte Spionage-Programme zu löschen, brauchen Sie ein echtes Antispyware-Programm wie „A-Squared free 3.0“ (auf Heft-CD/-DVD). So rücken Sie den Plagegeistern damit auf die Pelle:

1 Legen Sie die Heft-CD/-DVD ein, und klicken Sie anschließend auf **Titelthema**, auf **A-Squared free 3.0** und auf



Klicken Sie im nächsten Fenster auf **OK**, und folgen Sie den weiteren Anweisungen auf dem Bildschirm, um das Programm auf dem Computer einzurichten. Anschließend folgt ein Mausklick auf **Fertigstellen**.

2 Danach startet A-Squared automatisch und fragt, ob es sich auf den neuesten Stand bringen soll. Stellen Sie dann eine Internetverbindung her, und beantworten Sie die Frage mit einem Klick auf **Ja**.



3 Das Programm lädt daraufhin wichtige Aktualisierungen aus dem Internet. Ist der Vorgang abgeschlossen, erscheint die Meldung **Vorgang wurde erfolgreich abgeschlossen**. Als Nächstes starten Sie die Überprüfung des Computers. Dazu klicken Sie im Programmfenster

von A-Squared auf



damit der Eintrag orangefarben unterlegt erscheint: **Detail Scan**. Anschließend folgt ein Klick auf **SCAN**.

4 Der PC wird daraufhin gründlich nach Spionage-Software durchsucht. Das dauert ein paar Minuten. Schon während der Untersuchung listet A-Squared die gefundenen Schädlinge auf. Im Beispiel tauchen dabei auch Überbleibsel von Programmen auf, die im vorigen Abschnitt deinstalliert wurden, etwa



Warten Sie, bis der Fortschrittsbalken



verschwunden ist. Im Beispiel meldet A-Squared schließlich: **Gefundene Objekte: 60**.

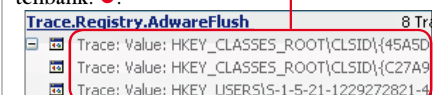
5 Es können aber je nach Computer auch weit aus mehr Schädlinge gefunden werden. Doch keine Panik! Viele der Funde sind vermutlich kein unmittelbares Risiko für den Computer. Relativ harmlos sind zum Beispiel **Cookies** (S.56) [02]. Wie gefährlich ein bestimmtes Objekt ist, steht direkt daneben, etwa

10 Traces - mittleres Risiko
5 Cookies - niedriges Risiko
1 Dateien - hohes Risiko

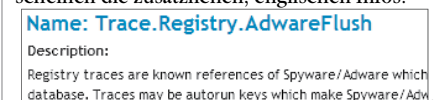
Detaillierte Informationen zum Schädling erhalten Sie jeweils nach einem Klick auf das kleine Pluszeichen **+** **Zeige alle gefundenen Objekte...** Im Beispiel zappelt das Schummel-Programm „Goodbye Spy“ im Netz:

Trace: c:\programme\goodbye spy\goodbytespy.exe

Viele Informationen helfen nicht gleich weiter, etwa solche Einträge in der Registrierungs-Datenbank:



In diesen Fällen finden Sie jedoch Hilfe im Internet. Klicken Sie dazu bei bestehender Internetverbindung auf die Überschrift, im Beispiel auf **Trace.Registry.AdwareFlush**. Kurz darauf erscheinen die zusätzlichen, englischen Infos:

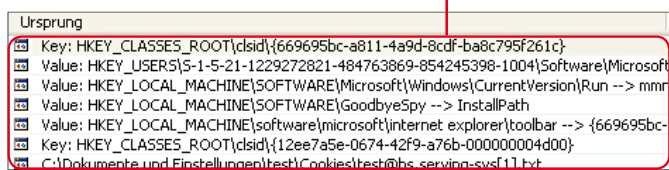


Fortsetzung

6 Schicken Sie alle entdeckten Schädlinge in die **Quarantäne** (S.56) 03, denn dort können Sie keinen Schaden anrichten. Um sämtliche Funde in einem Rutsch zu markieren, klicken Sie mit der **rechten** Maustaste auf einen Eintrag, etwa **Trace.TrackingCookie**, und wählen dann in der ausklappenden Liste per Klick **Alles selektieren** aus. Daraufhin werden alle Einträge mit einem Häkchen markiert, etwa



Klicken Sie auf **Ausgewähltes in Quarantäne**. Anschließend können Sie A-Squared mit einem Mausklick auf **Schließen** beenden.



7 Starten Sie dann Windows neu, und verwenden Sie den Computer am besten einige Tage wie gewohnt. Achten Sie dabei auf Probleme, die vorher nicht da waren. Starten Sie das Programm per Doppelklick auf



Nach einem Klick auf




erscheint eine Liste der „eingesperrten“ Schädlinge, hier

Jetzt gibt es mehrere Möglichkeiten:

■ Es gab keine Probleme beim Arbeiten: Dann löschen Sie die Schädlinge komplett. Klicken Sie dazu mit der **rechten** Maustaste in die Liste und anschließend auf **Alles selektieren**. Warten Sie einen Moment, bis alle Einträge grau hinterlegt sind. Klicken Sie auf **Löschen** und auf **Schließen**. Fertig.

■ Es gibt Probleme: Lässt sich ein bestimmtes Programm nicht mehr starten, oder stürzt es häufig ab? Dann stammt die zuvor gefundene Schadsoftware wahrscheinlich von diesem Programm. Sie sollten darauf künftig verzichten und es vom PC entfernen.

Haben Sie noch wichtige Daten, die Sie nur mit diesem Programm öffnen können? In diesem Ausnahmefall können Sie die Schädlinge für einen Noteneinsatz kurz „freilassen“. Trennen Sie dazu die Internetverbindung, und klicken Sie dann mit der **rechten** Maustaste in die Schädlingsliste. Im aufklappenden Menü wählen Sie den Eintrag **Alles selektieren** per Mausklick und klicken danach auf **Wiederherstellen**. Nach einem Neustart von Windows sollte die fehlerhafte Software wieder funktionieren. Aber denken Sie dran: Die Schädlinge sind jetzt wieder aktiv! Retten Sie deshalb sofort Ihre Daten. Anschließend wiederholen Sie die Anleitung, um die „befreiten“ Schädlinge gleich wieder einzufangen. Starten Sie dazu das Programm per Doppelklick auf  und die Aktualisierung mit einem Klick auf **Jetzt Updaten**. Weiter geht's mit Schritt 3.

Schritt 3: Registrierungs-Datenbank mit „CCleaner“ aufräumen

Auch wenn Sie Spionageprogramme mit A-Squared vernichten, kann es passieren, dass Reste in der Registrierungs-Datenbank übrig bleiben. Die sind zwar harmlos, aber sie machen Windows mit der Zeit langsamer. Von Hand sind solche Überbleibsel nur schwer aufzuspüren. Viel einfacher geht's mit „CCleaner 2.0“. Wie Sie das Programm nutzen, lesen Sie in den folgenden Schritten:

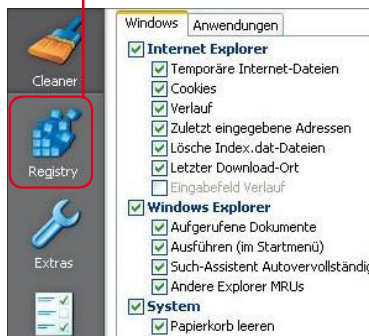
1 Öffnen Sie im Fenster der COMPUTERBILD-Heft-CD/DVD die Rubriken **Titelthema** und **CCleaner 2.0**. Klicken Sie dann auf **INSTALLIEREN**, und folgen Sie den weiteren Anweisungen auf dem Bildschirm. Entfernen Sie dabei das Häkchen ☒ **Füge CCleaner Yahoo! Toolbar hinzu**

mit einem Mausklick. Sobald das Programm installiert wurde, klicken Sie auf **Fertig stellen**.

2 Starten Sie nun CCleaner, zum Beispiel mit einem Doppelklick auf



Um die Registrierungs-Datenbank zu durchsuchen, klicken Sie im geöffneten Programmfenster auf



Lassen Sie die Voreinstellungen unverändert, und klicken Sie auf **Nach Fehlern suchen**. Der Vorgang kann nun eine Weile dauern. Nicht erschrecken: Beim ersten Suchvorgang findet CCleaner sehr viele überflüssige Einträge, zum Beispiel auch das „altbekannte“ Schummel-Antispionage-Programm

<input checked="" type="checkbox"/> ActiveX/COM Fehler	WMPPublihCntr.WMPPublihCntr.1 - {939438A9-CF0F-44d8-9140-
<input checked="" type="checkbox"/> Ungültiges Standardsymbol	%SystemRoot%\system32\appmgr.dll,-218
<input checked="" type="checkbox"/> ActiveX/COM Fehler	InProcServer32\{C:\WINDOWS\System32\plugin.ocx
<input checked="" type="checkbox"/> ActiveX/COM Fehler	InProcServer32\{C:\PROGRA~1\MESSEN~1\rtcmisp.dll
<input checked="" type="checkbox"/> Öffne mit Anwendung Problem	Applications\moviemk.exe\shell
<input checked="" type="checkbox"/> Anwendungspfad Fehler	cmmgr32.exe - C:\WINDOWS\System32\cmmgr32.exe
<input checked="" type="checkbox"/> Anwendungspfad Fehler	Pestbot.exe - C:\Programme\Pestbot\Pestbot.exe
<input checked="" type="checkbox"/> Fehlende MUI Beziehung	C:\Programme\SpywareSoftStop\SpywareSoftStop.exe
<input checked="" type="checkbox"/> Fehlende MUI Beziehung	C:\Programme\SpywareSoftStop\SpywareSoftStopUpdate.exe
<input checked="" type="checkbox"/> Fehlende MUI Beziehung	C:\DOKUME~1\test\LOKALE~1\Temp\is-KDJPC.tmp\is-COUVO.tmp
<input checked="" type="checkbox"/> Fehlende MUI Beziehung	C:\Programme\AdwareSpy\AdwareSpy4.exe

Um die Aufräumaktion zu starten, klicken Sie als Nächstes auf **Fehler beheben!**.

3 Das Programm CCleaner bietet die Möglichkeit, den Zustand der Registrierungs-Datenbank zum Zeitpunkt vor der Reinigung zu sichern. Sollte Windows nach der Putzaktion nicht mehr ordentlich funktionieren, können Sie das Betriebsprogramm damit ruck, zuck wiederherstellen. Beantworten Sie deshalb die Frage **Änderungen in der Registry sichern?** per Klick auf **Ja**. Wählen Sie dann einen Speicherort für die Sicherung aus, im Beispiel mit einem Mausklick auf



und einem Doppelklick auf **DATEN (H:)**. Klicken Sie anschließend auf die Schaltfläche **Speichern**. Jetzt folgen noch Mausklicks auf **Alle beheben** und **OK**. Sobald die Reinigung abgeschlossen ist, erscheint **Fehler beheben**. Es folgt ein Klick auf **Schließen**.

4 Manchmal entstehen durch die Reinigung weitere Reste. Wiederholen Sie deshalb die Prüfung. Klicken Sie auf **Nach Fehlern suchen**. Meldet CCleaner **Keine Fehler gefunden**, schließen Sie das Programm per Klick auf **X** und starten den PC neu. Andernfalls wiederholen Sie Schritt 3, um die Datenbank erneut aufzuräumen.

<input checked="" type="checkbox"/> ActiveX/COM Fehler	WMPPublihCntr.WMPPublihCntr.1 - {939438A9-CF0F-44d8-9140-
<input checked="" type="checkbox"/> Ungültiges Standardsymbol	%SystemRoot%\system32\appmgr.dll,-218
<input checked="" type="checkbox"/> ActiveX/COM Fehler	InProcServer32\{C:\WINDOWS\System32\plugin.ocx
<input checked="" type="checkbox"/> ActiveX/COM Fehler	InProcServer32\{C:\PROGRA~1\MESSEN~1\rtcmisp.dll
<input checked="" type="checkbox"/> Öffne mit Anwendung Problem	Applications\moviemk.exe\shell
<input checked="" type="checkbox"/> Anwendungspfad Fehler	cmmgr32.exe - C:\WINDOWS\System32\cmmgr32.exe
<input checked="" type="checkbox"/> Anwendungspfad Fehler	Pestbot.exe - C:\Programme\Pestbot\Pestbot.exe
<input checked="" type="checkbox"/> Fehlende MUI Beziehung	C:\Programme\SpywareSoftStop\SpywareSoftStop.exe
<input checked="" type="checkbox"/> Fehlende MUI Beziehung	C:\Programme\SpywareSoftStop\SpywareSoftStopUpdate.exe
<input checked="" type="checkbox"/> Fehlende MUI Beziehung	C:\DOKUME~1\test\LOKALE~1\Temp\is-KDJPC.tmp\is-COUVO.tmp
<input checked="" type="checkbox"/> Fehlende MUI Beziehung	C:\Programme\AdwareSpy\AdwareSpy4.exe

5 Sollte Windows nach dem Aufräumen nicht mehr funktionieren, starten Sie den PC im **abgesicherten Modus** (S.56) 04. Tippen Sie dazu beim Start mehrmals die **F8**-Taste. Danach tippen Sie so oft auf **F1**, bis **Abgesicherter Modus** markiert erscheint: **Abgesicherter Modus**. Drücken Sie dann die **↵**-Taste.

6 Wählen Sie als Nächstes den Speicherort der Sicherungsdatei. In diesem Beispiel folgen dazu Klicks auf **Start** und **Arbeitsplatz** sowie ein Doppelklick auf



Stellen Sie den „alten Zustand“ von Windows wieder her. Dazu klicken Sie im Beispiel doppelt auf die Datei **lcc 20071009 1339**, dann auf **Ja** und **OK**. Wiederholen Sie das gegebenenfalls mit der zweiten Sicherungsdatei. Starten Sie den PC anschließend neu.



Diese 122 Betrüger-Programme bedrohen Ihren PC

Der große COMPUTERBILD-Test zeigt: Immer mehr Programme im Internet geben sich als Gratis-Schutzsoftware aus, sind aber bloß ein Riesen-Schwindel. Die schlimmsten 122 Betrügerprogramme entlarvt diese Tabelle. Alle diese Gratisversionen sind nutzlos, da sie kaum Schädlinge aufspüren oder nur so tun. Einige sind sogar selbst Schädlinge und gefährden den PC.

COMPUTERBILD rät: Löschen Sie diese Programme sofort, falls Sie sie auf der Festplatte finden. Wie's geht, ist ab Seite 48 beschrieben. Dort steht auch, wie Sie das echte Anti-Spionage-Programm „A-Squared“ von der Heft-CD/-DVD verwenden. Zusammen mit dem Internet-Schutzpaket „Kaspersky Security Suite“ (ebenfalls auf Heft-CD/-DVD) schützt es Ihren PC.



Unterschiedliche Namen, gleiche Abzocke: AdwareStriker und SpyStriker ähneln sich bis ins Detail. Beide haben es nur auf Ihren Geldbeutel abgesehen.

Das richten die angeblichen Schutzprogramme an

Programmname der Gratisversion	Unerwünschte Datenrückstände nach Entfernung des Programms	Enthält Schädling	Erfindet Schädlinge	Erpresst zum Kauf der Bezahlversion	Ändert Windows-Dateien und/oder manipuliert das Internet-Zugriffsprogramm
100 Percent Anti-Spyware	mehrere Dateien	nein	nein	ja	nein
1 Click Spy Clean	Programmordner und Einträge in der Registrierungs-Datenbank sowie ein versteckter Startbefehl	nein	nein	ja	nein
Ad Armor	ein Programmordner, verschiedene DLL- und OCX-Dateien sowie mehrere Einträge in der Registrierungs-Datenbank	nein	nein	nein	ja
Ad-Purge Adware & Spyware Remover	Programmeinstellungen und DLL-Dateien sowie etwa 2000 Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
ADS Adware Remover	saubere Deinstallation	nein	nein	ja	nein
Adware Agent	saubere Deinstallation	nein	nein	ja	nein
AdwareBazooka	saubere Deinstallation	nein	ja	ja	ja
Adware Cops	DLL- und OCX-Dateien, sowie diverse Einträge in der Registrierungs-Datenbank	nein	nein	ja	ja
AdwareDelete	saubere Deinstallation	nein	nein	ja	ja
AdwareDeluxe (PCSafe Security Center)	ein Startmenü-Eintrag und eine DLL-Datei sowie Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
Adware Filter (PCSafe Security Center)	eine Programmdatei und Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
Adware Finder	saubere Deinstallation	nein	nein	nein	ja
AdwarePatrol	eine DLL-Datei sowie mehrere Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
AdwarePunisher	saubere Deinstallation	nein	ja	ja	ja
Adware Remover 1	eine DLL-Datei sowie mehrere Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
AdwareRemover 2	eine DLL-Datei sowie mehrere Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
AdwareSafety	ein Startmenü-Eintrag und eine DLL-Datei sowie zwei Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
AdwareSpy	Programmordner und eine Textdatei	nein	ja	ja	nein
AdwareStriker	mehrere DLL- und OCX-Dateien sowie Einträge in der Registrierungs-Datenbank	nein	ja	ja	ja
AlertSpy	eine Verknüpfung im Startmenü von Windows sowie eine DLL-Datei und verschiedene Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
AlfaCleaner	ein Programmordner, mehrere Konfigurationsdateien, mehrere Einträge in der Registrierungs-Datenbank sowie ein versteckter Startbefehl	nein	nein	ja	ja
AntiSpy Advanced	DLL-Datei	nein	ja	ja	nein
AntiSpyZone	Programmordner	nein	nein	ja	ja
AntiVermins (AntiVerminser)	Programmordner	nein	nein	ja	ja
Antivirgear	Programmordner und einige Dateien	nein	ja	ja	ja
AntiVirus Golden	Programmordner	nein	nein	ja	ja
AntiVirus Protector	DLL-Datei	nein	ja	ja	nein
Anti-Virus&Spyware	ein Programmordner und mehrere Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
ArmorWall	Einträge in der Registrierungs-Datenbank	nein	nein	ja	ja
BestGuardPlatinum	mehrere DLL-Dateien sowie verschiedene Einträge in der Registrierungs-Datenbank	nein	nein	ja	nein
BPS Spyware & Adware Remover	mehrere DLL- und OCX-Dateien sowie Einträge in der Registrierungs-Datenbank	nein	ja	ja	ja
Brave Sentry	Programmordner und -dateien, Startmenü-Einträge sowie Einträge in der Registrierungs-Datenbank	nein	nein	ja	ja
Clean Space	Programmdateien sowie verschiedene Einträge in der Registrierungs-Datenbank	nein	nein	ja	ja
CurePCSolution	Programmordner	nein	ja	ja	nein
Defenza	Programmordner und mehrere Dateien	nein	nein	ja	nein
Doctor Adware	eine DLL-Datei sowie verschiedene Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein

Das richten die angeblichen Schutzprogramme an

Programmname der Gratisversion	Unerwünschte Datenrückstände nach Entfernung des Programms	Enthält Schädling	Erfindet Schädlinge	Erpresst zum Kauf der Bezahlversion	Ändert Windows-Dateien und/oder manipuliert das Internet-Zugriffsprogramm
Doctor Adware Pro	eine DLL-Datei und verschiedene Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
Easy SpyRemover	ein Programmordner und ein versteckter Starteintrag in der Registrierungs-Datenbank	nein	nein	ja	nein
Errorsafe	Programmordner und -dateien	nein	ja	ja	nein
ETD Security Scanner	Programmordner, mehrere Textdateien, Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
ExpertAntiVirus	Programmordner, ein Schädling, Einträge in der Registrierungs-Datenbank	ja	ja	ja	ja
Froggie Scan	Programmordner, eine OCX-Datei, Einträge in der Registrierungs-Datenbank	nein	ja	nein	nein
GoodbyeSpy	ein Programmordner und mehrere Einträge in der Registrierungs-Datenbank	nein	ja	nein	nein
Internet Cleanup	Programmordner, mehrere Dateien und Einträge in der Registrierungs-Datenbank	nein	nein	nein	ja
KaZaaP	verschiedene Einträge in der Registrierungs-Datenbank von Windows	nein	ja	ja	nein
MalwareAlarm	Programmordner und zwei Programmdateien	nein	nein	ja	ja
MalwareScanner	eine DLL- und eine OCX-Datei, Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
MalwareWipe/MalwareWiper/MalwareWiped	Programmordner	nein	nein	ja	nein
MaxNetShield (MNS Spyware Remover & History Eraser)	ein Programmordner und mehrere Einträge in der Registrierungs-Datenbank	nein	nein	nein	ja
MySpyProtector	ein Programmordner und mehrere Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
MyNetProtector	Programmordner	nein	ja	ja	ja
One-Shot Antivirus	lässt sich nicht deinstallieren	ja	nein	nein	ja
PAL Spyware Remover	Programmordner, OCX-Dateien, Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
PC Health Plan	Programmordner und Prüfprotokolle	nein	ja	ja	nein
pcOrion	Programmordner, zwei OCX-Dateien sowie Einträge in der Registrierungs-Datenbank	nein	nein	ja	ja
PestBot	eine DLL-Datei sowie verschiedene Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
PestProtector	ein Startmenüeintrag, eine DLL-Datei und zwei Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
Privacy Defender	Einträge in der Registrierungs-Datenbank	nein	ja	nein	nein
RazeSpyware	saubere Deinstallation	nein	ja	ja	ja
Real AdWareRemoverGold	mehrere DLL- und OCX-Dateien sowie Einträge in der Registrierungs-Datenbank	nein	nein	ja	ja
RegFreeze	Einträge in der Registrierungs-Datenbank	nein	nein	ja	nein
Registry_Doctor	Programmordner	nein	ja	ja	nein
RemedyAntiSpy	saubere Deinstallation	nein	ja	ja	nein
RemoveIT Pro	ein versteckter Starteintrag und Einträge in der Registrierungs-Datenbank	nein	nein	ja	ja
Rosecitysoftware	ein Programmordner und mehrere Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
Safe & Clean (Scan & Clean)	ein versteckter Starteintrag und Einträge in der Registrierungs-Datenbank	nein	ja	ja	ja
ScanSpyware	saubere Deinstallation	nein	ja	ja	nein
SecureMyPC	saubere Deinstallation	nein	ja	ja	ja
Securitysuite	ein Programmordner sowie mehrere Einträge in der Registrierungs-Datenbank	nein	nein	ja	nein
SpyAdvanced	eine DLL-Datei und verschiedene Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
SpyBouncer	mehrere OCX-Dateien sowie mehrere Einträge in der Registrierungs-Datenbank	nein	nein	ja	nein
SpyCleaner	Programmordner, einige OCX-Dateien, Einträge in der Registrierungs-Datenbank	nein	ja	nein	nein
SpyCrush	Programmordner	nein	nein	ja	nein
SpyCut	saubere Deinstallation	nein	ja	ja	ja
SpyDawn	Programmordner	nein	nein	ja	nein
SpyDestroy Pro	eine DLL-Datei sowie mehrere Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
SpyEliminator	mehrere DLL- und OCX-Dateien sowie Einträge in der Registrierungs-Datenbank	nein	ja	ja	ja
SpyFighter	Programmordner und mehrere Dateien, ein versteckter Starteintrag sowie Einträge in der Registrierungs-Datenbank	nein	nein	ja	nein
SpyHeal	Programmordner und -datei sowie Einträge in der Registrierungs-Datenbank	nein	nein	ja	nein

Das richten die angeblichen Schutzprogramme an

Programmname der Gratisversion	Unerwünschte Datenrückstände nach der Entfernung der Software	Enthält Schädling	Erfindet Schädlinge	Erpresst zum Kauf der Bezahlversion	Ändert Windows-Dateien und/oder manipuliert das Internet-Zugriffsprogramm
SpyiBlock	ein versteckter Starteintrag	nein	ja	ja	ja
Spy-Kill	saubere Deinstallation	nein	nein	ja	nein
Spy Killer	Einträge in der Registrierungs-Datenbank	nein	nein	ja	nein
SpyKillerPro	Programmordner	nein	nein	ja	ja
SpyLax	Programmordner und -datei, mehrere OCX-Dateien sowie Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
SpyLocked	Programmordner	nein	nein	ja	nein
SpyNoMore	eine Systemdatei, ein versteckter Starteintrag und Einträge in der Registrierungs-Datenbank	nein	nein	ja	nein
SpyOnThis	Programmordner	nein	ja	ja	nein
SpyPry	Programmordner, einige Dateien, Einträge in der Registrierungs-Datenbank	nein	ja	nein	nein
SpyRemover	diverse Einträge in der Registrierungs-Datenbank	nein	ja	ja	ja
SpySheriff	Programmordner und diverse Programmdateien, Einträge in der Registrierungs-Datenbank	nein	nein	ja	ja
SpyShield	Programmordner, eine OCX-Datei sowie diverse Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
Spy Sniper	Programmordner, eine OCX-Datei und Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
SpyStriker	eine DLL- und eine OCX-Datei sowie Einträge in der Registrierungs-Datenbank	nein	ja	ja	ja
SpyViper	Programmordner, eine OCX-Datei und Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
Spyware & Adware Removal	Einträge in der Registrierungs-Datenbank	nein	Nein	nein	nein
Spyware Annihilator	Programmordner und diverse Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
SpywareBeGone	Programmordner und diverse Dateien, Einträge in der Registrierungs-Datenbank mit verstecktem Starteintrag	nein	nein	nein	ja
Spyware Cops	eine DLL- und OCX-Datei sowie Einträge in der Registrierungs-Datenbank	nein	nein	ja	nein
SpywareCrusher	Programmordner, eine OCX-Datei und Einträge in der Registrierungs-Datenbank	nein	nein	ja	nein
Spyware Quake	ein Programmordner, diverse Dateien und eine Verknüpfung im Startmenü von Windows	nein	nein	ja	nein
SpwareRemoval	eine DLL-Datei sowie verschiedene Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
Spyware Remover 1	eine Programmdatei	nein	nein	nein	ja
Spyware Scrapper	eine OCX-Datei sowie diverse Einträge in der Registrierungs-Datenbank	nein	nein	ja	nein
SpyWare Secure	saubere Deinstallation	nein	nein	ja	nein
Spyware Soft Stop	diverse Programm-, DLL- und OCX-Dateien, mehrere versteckte Starteinträge und diverse weitere Einträge in der Registrierungs-Datenbank	ja	ja	ja	ja
Spyware Striker Pro	Programmordner und diverse Programmdateien, Einträge in der Registrierungs-Datenbank	nein	nein	ja	ja
SpywareTek/Spyware Removal System	saubere Deinstallation	nein	ja	ja	ja
SpywareXP	eine DLL-Datei sowie mehrere Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
SpywareZapper	eine DLL- und OCX-Datei sowie diverse Einträge in der Registrierungs-Datenbank	nein	nein	ja	nein
StartGuard	eine OCX-Datei und verschiedene Einträge in der Registrierungs-Datenbank	nein	ja	nein	nein
Super Spyware Remover	Programmordner	nein	ja	nein	nein
The SpyGuard	saubere Deinstallation	nein	ja	ja	ja
TrueSword4	Programmordner und diverse Einträge in der Registrierungs-Datenbank	nein	nein	ja	nein
Trust Cleaner	Programmordner, eine Steuerungsdatei („Treiber“) sowie verschiedene versteckte Starteinträge	nein	ja	ja	ja
Ultimate Defender	mehrere geschützte Dateien	nein	ja	ja	nein
VirusBlast	Programmordner und Programmdateien sowie Einträge in der Registrierungs-Datenbank	nein	nein	ja	ja
VirusRescue	ein Programmordner sowie mehrere Einträge in der Registrierungs-Datenbank	nein	nein	ja	ja
Winkeeper	eine Textdatei und verschiedene Einträge in der Registrierungs-Datenbank	nein	nein	nein	ja
WinSOS	Programmordner und mehrere Programmdateien sowie verschiedene Einträge in der Registrierungs-Datenbank	nein	ja	nein	nein
Wiperwiz	saubere Deinstallation	nein	ja	ja	nein
X-Con Spyware Destroyer	ein Programmordner und zwei Einträge in der Registrierungs-Datenbank	nein	ja	ja	nein
ZoneProtect AntiSpyware	ein Programmordner, diverse DLL- und OCX-Dateien, ein versteckter Starteintrag und einige weitere Einträge in der Registrierungs-Datenbank	nein	nein	nein	ja

So testet COMPUTERBILD

Ob ein vorgebliches Schutzprogramm nutzlos ist, erpresserisch beworben wird oder sogar schädliche Software enthält, untersuchte COMPUTERBILD zusammen mit den Computerviren-Experten der Otto-von-Guericke-Universität Magdeburg und dem unabhängigen Testlabor AV-Test.

Der Testaufbau

Ein Team von sechs Testern machte sich im Internet auf die Suche nach den betrügerischen Programmen. Aus Leserhinweisen sowie Einträgen in Foren und auf speziellen Internetseiten zum Thema Sicherheit ergab sich nach einigen Tagen Recherche eine Liste mit 122 verdäch-

überprüfte, ob und welche Daten die Betrüger-Programme von den Testcomputern ins Internet sendeten.

■ Was richtet ein gestartetes Betrüger-Programm eigentlich auf dem Computer an? Um das zu ermitteln, verwendeten die Tester die Spezialsoftware „Olly Dbg 1.10“. Dieses Werkzeug überwacht jeden einzelnen Programmschritt und hilft, die Funktionsweise zu verstehen. Das funktioniert etwa so, als würden Sie einen Sportler in Zeitlupe betrachten und ihn dabei röntgen.

Mit weiteren Hilfsprogrammen protokollierte das Team jede Veränderung auf der Festplatte und in der Registrierungs-Datenbank.

dem Internet überspielt. Schon während der Übertragung und dann noch einmal vor der Installation überprüften Antiviren- und Anti-Spionage-Programme sämtliche Daten auf Schädlinge.

Schritt 2: Das Betrüger-Programm wurde gestartet. Die Tester untersuchten den Umfang des Betrugs:

- Installiert es echte Schadprogramme, um sie dann zu melden?
- Meldet es Schädlinge, die gar nicht vorhanden sind?
- Erpresst es den arglosen Anwender zum Kauf einer Vollversion?
- Manipuliert das Betrüger-Programm das Internet-Zugriffsprogramm und schafft damit möglicherweise Sicherheitslücken?

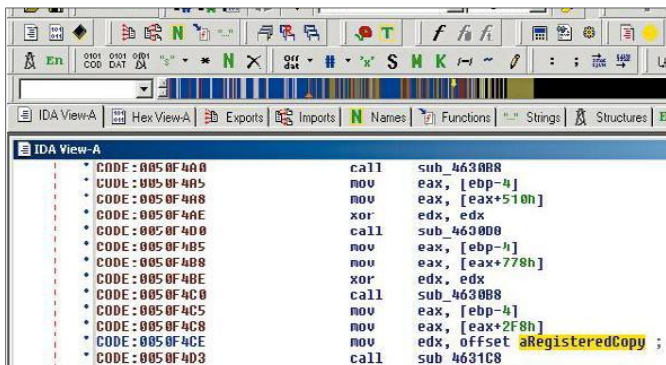
Während dieser Untersuchung wurden die Betrüger-Programme von den Antiviren- und Anti-Spionage-Programmen und von Olly Dbg auf Manipulationen überwacht. Zusätzlich kontrollierte Wireshark Datenübertragungen ins Internet.



Den Betrügern auf der Spur: Das Team von AV-Test nahm 122 gefährliche Programme unter die Lupe.

Schritt 3: Anschließend deinstallierten die Tester die Betrüger-Programme mit Windows-Bordmitteln. Dann untersuchten sie die Festplatte auf Dateireste und überprüften, ob noch lauffähige Bestandteile zurückgeblieben waren. Denn die könnten ein Hinweis auf Viren und Trojaner sein.

Schritt 4: Alle Kandidaten, die in den Schritten zuvor auffällig wurden, gingen in eine weitere Testrunde. Nach der erneuten Installation des Betrüger-Programms kontrollierten die Tester mit der Software Datarescue jede Aktivität während des Programmablaufs. So kamen die Tester auch besonders trickreichen Manipulationen auf die Spur.



Überwachung des Programmablaufs: Hier analysiert „Olly Dbg“, was ein Betrüger-Programm nach dem Start auf dem PC tatsächlich tut.

tigen Programmen. Zur Vorbereitung des Tests wurden 50 identisch ausgestattete Windows-XP-Computer aufgestellt. Jeder war ausgerüstet mit einem Paket von Test- und Prüfsoftware. Darin enthalten: die von der COMPUTERBILD-Heft-CD/-DVD bekannte „Kaspersky Security Suite“ sowie die Anti-Spionage-Programme „Spybot S & D 1.5“, der „Windows-Defender“, „Ad-Aware 2007“ und „A-Squared 3.0“. Der Sinn der mehrfachen Absicherung: Nicht jedes Schutzprogramm entdeckt jeden Schädling.

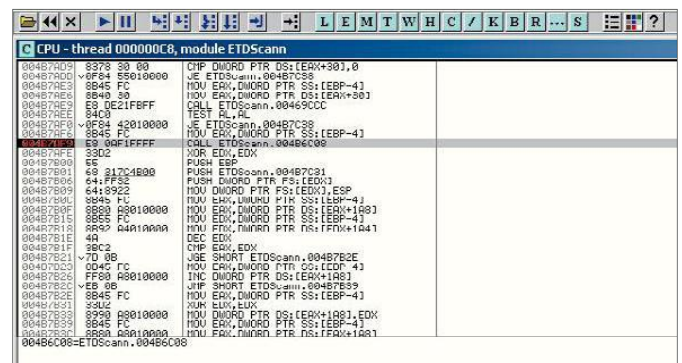
■ Auf einem weiteren Computer ließen die Tester das Überwachungsprogramm „Wireshark“ laufen. Das

steckt in einem Betrüger-Programm möglicherweise noch mehr Gefahrenpotenzial, das nur im Moment noch nicht sichtbar ist? Das wurde in jedem Verdachtsfall mit einer noch genaueren Analyse untersucht. Mit dem Spezialprogramm „Datarescue IDA Pro 4.8“ lässt sich das Betrüger-Programm in seine Bestandteile zerlegen. Jeder einzelne Programmschritt kann so entschlüsselt werden.

Testablauf

Der Test der Betrüger-Programme lief in drei Schritten ab:

Schritt 1: Von allen Programmen wurden die Gratisversionen aus



Bringt ein Betrüger-Programm den Computer mit versteckten Kniffen in Gefahr? Mit „Datarescue IDA Pro“ untersuchten die Tester die Einzelbestandteile der Abzock-Software.

WAS IST EIGENTLICH?

01 Registrierungs-Datenbank

In dieser Datei („Registry“) speichert Windows die meisten Einstellungen. Darin steht etwa, welche Software auf welche Daten zugreift. Falsche Einträge können dazu führen, dass Windows nicht startet. Sie können die

Registrierungs-Datenbank mit dem Hilfsprogramm „Regedit“ bearbeiten:



02 Cookies

Cookies sind Textinformationen, die von Internetangeboten auf dem Computer gespeichert werden. Sie enthalten etwa Ihre Zugangsdaten zu Internetläden, Ihren Warenkorb oder eine Liste der Seiten, die Sie im Internet besucht haben.

03 Quarantäne

Eine vorübergehende Isolation zur Verhinderung der Krankheitsausbreitung gibt es auch am PC: Dabei werden Schadprogramme in einen geschützten Bereich verschoben. Dadurch lassen sich vor dem nötigen Löschen gegebenenfalls noch Daten retten.

04 Abgesicherter Modus

Der „abgesicherte Modus“ ist eine Art Noteingang für Windows XP und Vista. Falls der PC nicht mehr normal starten kann, lassen sich in dieser Betriebsart Fehler beheben. Zum Beispiel blockierende Programme wieder von der Festplatte entfernen.

05 DLL-/OCX-Dateien

DLL-Dateien sind Bibliotheken. Sie enthalten Programmbestandteile („Unterprogramme“), die sich von anderen Programmen aus nutzen lassen. OCX-Dateien sind spezielle Bibliotheken, die häufig der Internet Explorer nutzt.

*Weitere Fachbegriffs-Erklärungen auf Seite 192/193