Das gab's noch nie: In einer deutschlandweiten Aktion machen die Bundesregierung, COMPUTERBILD und weitere Partner gegen Botnetze mobil. Als COMPUTERBILD-Leser können Sie als Erste dabei sein und Ihren PC von Bots befreien. Dazu exklusiv im Heft: Die offizielle Anti-Bot-CD!

Es herrscht Krieg im Internet. Kriminelle haben eine gigantische Streitmacht mit Millionen gekaperter Computer aufgestellt. Raffinierte Schädlinge machen immer mehr Privat-PCs zu willenlosen Robotern, kurz: „Bots*". Als Teil eines Botnetzes versenden die Computer selbst massenweise Viren und Spam oder attackieren gar staatliche Computernetze und Wirtschaftsunternehmen. Der Nutzer merkt aber gar nicht, dass sein PC für Straftaten missbraucht wird.

Mittlerweile stammen rund 95 Prozent aller Spam-Mails von Botnetzen. Wie Bots funktionieren, lesen Sie auf Seite 42.

Die Anti-Bot-Initiative

Damit Sie herausfinden können, ob Ihr PC ohne Ihr Wissen ein Doppelleben führt, hat eine neue Initiative eine Waffe gegen diese Roboter-Viren entwickelt. Ab 15. September beginnt die Offensive mit der Internetseite www.botfrei.de. Große Internetanbieter arbeiten dort in einem ausgeklügelten System zusammen. Fällt der PC eines ihrer Kunden als botinfiziert auf, erhält der Nutzer eine Benachrichtigung, die Hilfestellung gegen die Bedrohung bietet.

Wie das funktioniert und ob Ihr Internetanbieter schon Mitglied dieser Allianz ist, steht auf Seite 43.

COMPUTERBILD-Leser müssen aber nicht auf schlechte Nachrichten warten, sondern können mit der Anti-Bot-CD ihren PC schon jetzt auf Bots überprüfen:

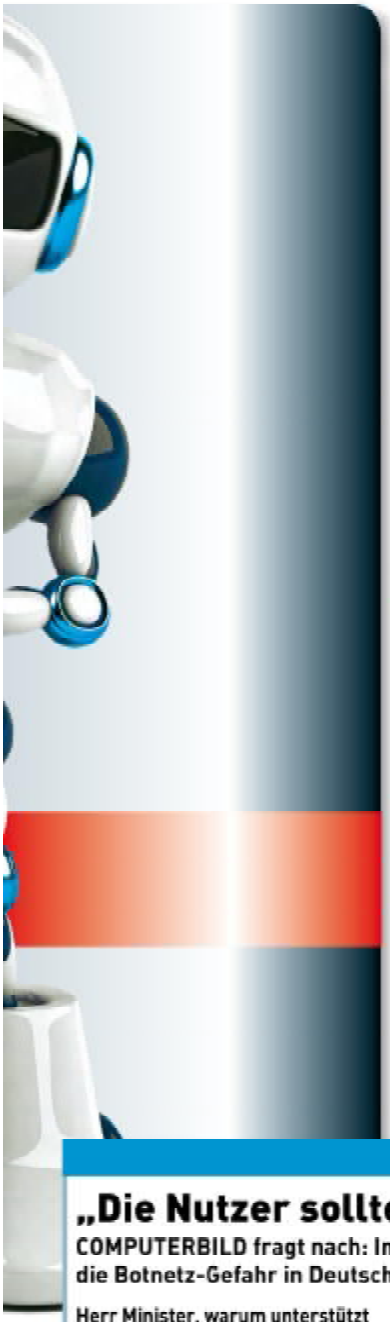
Wer hat die Anti-Bot-CD entwickelt?

Das DE-Cleaner Rettungssystem auf der CD hat eine schlagkräftige Allianz entwickelt:

- **Das Bundesamt für Sicherheit in der Informationstechnologie (BSI):** Das Bundesamt ist für die Sicherheit im Internet zuständig. Es koordiniert die Verwendung der 2 Millionen Eu-

So einfach war der Kampf gegen Bots noch nie: Anti-Bot-CD einlegen, Computer prüfen und Schädlinge ganz einfach löschen. Wie's geht, steht auf Seite 44.

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 132/133.



Das Anti-Botnet Beratungszentrum startet am 15. September unter der Adresse www.botfrei.de. Die Bundesregierung unterstützt das Projekt mit 2 Millionen Euro.

ro, die das Bundesinnenministerium für den Kampf gegen Botnetze bereitstellt. Die BSI-Experten haben das DE-Cleaner Rettungssystem auf Herz und Nieren geprüft.

- **Der Verband der deutschen Internetwirtschaft e.V. (eco):** Im eco-Verband sind die meisten deutschen Internet-Zugangsanbieter organisiert. Eco betreibt das neue Anti-Botnet-Beratungszentrum botfrei.de und verteilt darüber auch das DE-Cleaner Rettungssystem.
- **Avira:** Für die Anti-Bot-CD stellt der Virenspezialist Avira die Technik zur Verfügung, die Bots identifizieren und abschalten kann.
- **COMPUTERBILD:** Die Experten von COMPUTERBILD haben die gesamte Nutzeroberfläche des DE-Cleaner Rettungssystems entwickelt.

Ziel dieser einzigartigen Kooperation: Das Internet soll wieder sicherer werden und Deutschland endlich seinen Spitzenplatz der botverseuchten Länder Europas verlieren.

Was kann die Anti-Bot-CD?

Das DE-Cleaner Rettungssystem spürt Bots auf Ihrem Computer auf und vernichtet sie. Die weiteren Vorteile:

- Sie starten Ihren Computer direkt von der Anti-Bot-CD. Sie kann – im Gegensatz zum normalen Virenschutz-Programm – auch Schädlinge abschalten, die sich bei laufendem Windows nicht löschen lassen.
- Das System kommt Ihrem Virenschutz-Programm auf gar keinen Fall in die Quere. So kann jeder PC-Nutzer die Anti-Bot-CD zusätzlich verwenden.
- Sie können das Rettungssystem auch auf Netbooks ohne CD-Laufwerk nutzen. Denn das DE-Cleaner Rettungssystems lässt sich auch auf einem USB-Stift* installieren und von dort starten.
- Das DE-Cleaner Rettungssystem bleibt immer auf dem neuesten Stand. Aktuelle Informationen über Bots holt es sich aus dem Internet.

Interview

„Die Nutzer sollten mehr tun“

COMPUTERBILD fragt nach: Innenminister Thomas de Maizière über die Botnetz-Gefahr in Deutschland und die Verantwortung der Bürger

Dr. Thomas de Maizière
Bundesinnenminister

Herr Minister, warum unterstützt der Staat die Bekämpfung von Botnetzen mit Millionen von Euro?
Botnetze sind aktuell die größte Gefährdung für das Internet und die daran angeschlossenen Infrastrukturen. Hier besteht dringender Handlungsbedarf. Betroffen sind auch die Bürger, die das Internet über Service Provider benutzen. Viele Nutzer merken es oft gar nicht, dass ihr Computer bereits infiziert ist. Hier setzt das Projekt an. Die Provider können den Bürgern helfen, sich sicher durch das Internet zu bewegen. Dies unterstützt der Staat mit einer Anschubfinanzierung von 2 Millionen Euro für eine privatwirtschaftliche Initiative zur Bekämpfung von Botnetzen.

Wie gefährlich sind Botnetz-Attacken für die Computersysteme der Regierung oder der Wirtschaft?
Nach Schätzungen sind Millionen Computer in Botnetze eingebunden. Wenn Kriminelle die Rechenleistung vieler fremder Computer bündeln und private Netzwerke oder staatliche Computersysteme attackieren, kann dies zu schwerwiegenden Schäden führen. Die Bundesregierung unternimmt erhebliche Anstrengungen, um ihre Computernetze zu schützen.

Kann der Nutzer nicht selbst für Sicherheit sorgen?
Ja, die Nutzer sollten mehr tun. Sie können es auch, etwa durch den Einsatz einer Firewall* und eines Virenscanners, die auf dem aktuellen Stand sind. Wichtig ist außerdem, dass die Nutzer die von den Herstellern des Betriebssystems* und der Anwendungssoftware bereitgestellten Updates zeitnah einspielen.

In anderen Ländern werden botinfizierte Computer gar nicht mehr ins Internet gelassen. Drohen den deutschen Internetsurfern auch solche Maßnahmen?
Das Sperren von infizierten Computern ist im Rahmen des Projekts nicht vorgesehen. Es bleibt wie bisher den Service Providern überlassen, wie sie die Geschäftsbedingungen ausgestalten.

ZAHLEN RUND UM BOTNETZE

BOT-VERSEUCHUNG IN EUROPA IM VERGLEICH

1. DEUTSCHLAND
2. ITALIEN
3. SPANIEN
4. POLEN
5. TÜRKEI
6. FRANKREICH

Quelle: Symantec

12,7 MILLIONEN

PCs umfasste das bisher größte entdeckte Botnetz „Mariposa“. Es war auf den Diebstahl von Kreditkarten- und Homebanking-Daten spezialisiert. Anfang März 2010 wurden die spanischen Betreiber des Netzes verhaftet. Im Juli folgte die Festnahme der Programmierer, die die Botnetz-Software hergestellt hatten.

122 MILLIARDEN

unerwünschte und teils gefährliche E-Mails werden täglich durch Botnetze verschickt. Das sind etwa zwei Drittel des weltweiten E-Mail-Aufkommens.

DIE FÜNF GRÖSSTEN BOTNETZE

1. 13 MIO. PCs MARIPOSA
2. 9 MIO. PCs CONFICKER
3. 1,5 MIO. PCs RUSTOCK
4. 1,1 MIO. PCs GRUM
5. 0,7 MIO. PCs CUTWAIL

70 US-DOLLAR (55 Euro)

zahlen Kriminelle auf dem Schwarzmarkt für eine 24-stündige Botnetz-Attacke auf die Internetseite eines Kleinunternehmens. Die Seite des Unternehmens ist in dieser Zeit für niemanden erreichbar. Skrupellose Konkurrenten setzen so gezielt ihre Mitbewerber außer Gefecht.

37 290 US-DOLLAR (circa 29 000 Euro)

erhielt ein 19-jähriger Krimineller aus den Niederlanden für den Verkauf des Botnetzes „Shadow-Botnet“, das er zuvor aufgebaut hatte. Ein Brasilianer kaufte die Kontrolle über das Netz, für das rund 100 000 PCs gekapert worden waren.

SO FUNKTIONIEREN BOTNETZE

Schon der Besuch einer harmlosen Internetseite kann Ihren PC verseuchen und in einen Bot verwandeln. Kriminelle platzieren die dazu nötigen Trojaner* nicht mehr nur auf dubiosen oder halbseidenen Internetseiten. Immer häufiger schieben sie Schädlinge auch seriösen Angeboten mit vielen Besuchern unter, zum Beispiel Online-Magazinen oder den Hilfe-Seiten von PC-Herstellern.
Um auf den PC des Opfers zu gelangen, nutzen die Schädlinge Sicherheitslücken. Dazu zählen veraltete Versionen von Windows, dem Browser und Adobe Reader, ein veralteter oder deaktivierter Virenschutz sowie der arglose Umgang mit E-Mails.

So wird Ihr PC zum Botnetz-Sklaven

1 MANIPULATION

Der Angreifer bricht in eine gut besuchte Internetseite ein und platziert dort einen Schädling, etwa in einem Werbebanner.

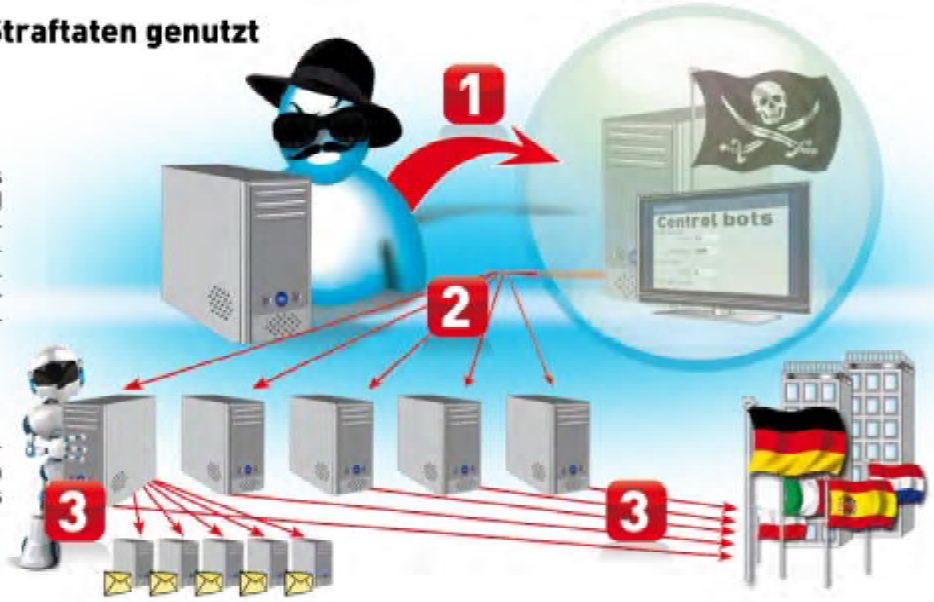
2 INFEKTION

Das Opfer besucht die manipulierte Seite. Hat sein PC eine passende Schwachstelle, wird er infiziert („Drive-by-Download").

3 FEINDLICHE ÜBERNAHME

Der Schädling richtet die Bot-Software ein, die mit dem „Botnetz-Conroller" (siehe unten) Kontakt aufnimmt und auf Befehle wartet. Zusätzlich werden oft weitere Programme installiert: Über ein **Hintertür-Programm** erlangt der Anreifer die vollständige Kontrolle über den PC, **Spionage-Software** erschnüffelt etwa Passwörter und sendet sie zum Angreifer, oder der PC wird als **Umleitung** für den Besuch illegaler Internetseiten missbraucht.

So wird Ihr PC für Straftaten genutzt



1 TARNUNG

Die Software zur Verwaltung des Botnetzes („Botnetz-Controller") liegt meist auf einem gekaperten Internet-Server*. Durch Verschleierung seiner Internet-Kennung (IP-Adresse) ist der Server getarnt. Der Angreifer bleibt dadurch im Hintergrund.

2 BEFEHL

Der Gauner meldet sich am Botnetz-Controller an und erteilt in einem Rutsch allen Sklaven-PCs den Angriffsbefehl.

3 ANGRIFF

Die Sklaven führen den Befehl aus. Es gibt zwei Formen:

- **DDoS-Attacke (Distributed Denial of Service):** Alle Bots überhäufen einen bestimmten Internet-Server mit sinnlosen Anfragen, um ihn zu überlasten. Dies wird häufig genutzt, um Internetseiten von Wirtschaft und Politik lahmzulegen.
- **Spam-Versand:** Jeder Bot-PC verschickt heimlich E-Mails, zum Beispiel an die Outlook-Kontakte des ahnungslosen Besitzers. Oft führen die Links* in diesen E-Mails zu betrügerischen Internetseiten („Phishing"), zu Schadsoftware oder wieder zu der manipulierten Internetseite, die schon den Absender infizierte.

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite XXX/XXX. [1]COMPUTERBILD hat die „04_Fussnote" neu erfunden und mit der CB DIN Condensed Regular 7,5 auf 9 definiert.
[2]Die hochgestellten Ziffern haben das Zeichenformat 04_Fussnote_HOCH. [3]Preis gilt für Anrufe aus dem deutschen Festnetz, vom Handy je nach Anbieter teurer.

SO FUNKTIONIERT DER KAMPF GEGEN BOTNETZE

Am 15. September startet die Aktion gegen Botnetze. Dann benachrichtigen die ersten Internet-Zugangsanbieter die Besitzer von Sklaven-PCs – woran sie diese erkennen, steht im Kasten unten auf dieser Seite. In den Mitteilungen erfahren die Betroffenen, wie sie gegen die Verseuchung des PCs vorgehen (Schritte 1 bis 4 unten). COMPUTERBILD-Leser haben's leichter: Sie können gleich die Desinfektions-CD nutzen.

So funktioniert das neue Anti-Bot-System

1 BENACHRICHTIGUNG DES ANBIETERS

Mit Start der Anti-Bot-Aktion am 15. September versenden die ersten Internetanbieter Benachrichtigungen an Kunden, deren Computer Bot-verseucht sind. Je nach Anbieter werden die Betroffenen per Brief, E-Mail, SMS, Telefon oder vorgeschalteter Internetseite im Browser verständigt.
Die Benachrichtigung enthält in jedem Fall diese Informationen:
- Verweis auf die Internetseite „botfrei.de",
- eventuell Telefonnummer und Zugangscode für die „botfrei.de"-Hotline.

2 BESUCH DER SEITE „BOTFREI.DE"

Auf dieser Internetseite können sich Betroffene über Botnetze, die Schritte zur Desinfektion des PCs und zur Vorsorge informieren. Hier lässt sich zunächst zwar nicht das komplette Rettungssystem, aber das Prüfprogramm DE-Cleaner von Symantec herunterladen und ohne Installation direkt starten.

3 ONLINE-PRÜFPROGRAMM NUTZEN

Die Symantec-Software untersucht den Computer auf Botnetz-Befall und versucht, den PC zu desinfizieren. Da sich Schädlinge im laufenden Windows-Betrieb besonders gut tarnen können, werden möglicherweise nicht alle erkannt und gelöscht. Es kommt dann zur Fehlermeldung oder zum Abbruch.

4 ANBIETER-HOTLINE

Während bei Versatel die Teilnahme an der „botfrei.de"-Hotline noch nicht sicher ist, wollen Netcologne und T-Online ihre Kunden an die eigenen Hotlines verweisen.
versatel: 0800/333 444 8
NETCOLOGNE: 0800/2222-8000
T-Online: 0800/330-1000

4 „BOTFREI.DE"-HOTLINE

Kann das Prüfprogramm den PC nicht desinfizieren, hilft die Hotline von „botfrei.de" weiter. Telefonnummer und Zugangscode erhalten Kunden von osc, Kabel BW und 1&1 in Schritt 1. Bei Bedarf verschickt die Hotline das DE-Cleaner Rettungssystem (siehe oben) als CD oder als Datei zum Brennen.

So einfach haben es COMPUTERBILD-Leser

Computer Bild-LESER
MIT DE-CLEANER
RETTUNGS-CD

Sie haben die CD- oder DVD-Ausgabe von COMPUTERBILD? Dann können Sie sich alle anderen Schritte sparen und gleich mit der Bot-Beseitigung loslegen. Das DE-Cleaner Rettungssystem lässt sich auch ohne Internetanbieter-Benachrichtigung vorbeugend zur Bot-Erkennung verwenden.
Das DE-Cleaner Rettungssystem startet den PC ohne Windows. So gelingt ihm eine gründlichere Schädlingserkennung. Wie's funktioniert, erfahren Sie Schritt für Schritt ab Seite 44.

IST IHR PC INFIZIERT? SO ERMITTELN DIE INTERNETANBIETER

Die Internet-Zugangsanbieter wie 1&1 und T-Online werden ständig Zeugen von Botnetz-Angriffen: Entweder weil ihre eigenen Server oder die ihrer Firmenkunden Angriffsziele sind. Da auch die Besitzer der angreifenden Sklaven-PCs zu den Kunden zählen, können die Anbieter sie anhand der IP-Adresse identifizieren.

ANGRIFFSAUSWERTUNG

Damit ein Computer einen anderen PC angreifen kann, muss er dessen IP-Adresse kennen. Die erhält der Angreifer von einem Verzeichnis-Server im Internet, der wie eine Vermittlungsstelle arbeitet. Da solche Server meistens Internetanbietern gehören, registrieren diese die auffälligen Anfragen und IP-Adressen der Angreifer und vergleichen sie mit denen ihrer Kunden.

SPAMTRAPS

Spamtraps (Werbe-Fallen) sind geheime E-Mail-Adressen, die Anbieter auf ihren Internetseiten verstecken, zum Beispiel in weißer Schrift auf weißen Internetseiten. Für Menschen unsichtbar sammeln Roboter-Programme diese Adressen im Auftrag der Werbe-Versender ein. Schickt nun ein Privat-PC eine E-Mail an eine solche Adresse, ist klar, dass dieser PC infiziert ist. Dessen IP-Adresse muss der Anbieter nur noch mit seinen Kundendaten abgleichen.

HONEYPOTS

Honeypots (Honigtöpfe) sind PCs ohne Sicherheitssoftware und Windows-Updates, die ständig mit dem Internet verbunden sind. Ihr einziger Zweck: Sie sollen angegriffen werden. Sobald das geschieht, ermittelt der Anbieter die Art des Schädlings und die IP-Adresse des Angreifers.

SINKHOLES

Gelegentlich können Polizei und Anbieter die Server der Botnetz-Betreiber im Internet enttarnen und unter ihre Kontrolle bringen. Solche gekaperten Server werden dann als Sinkhole (Senkgrube) bezeichnet. Da sich die Sklaven-PCs weiterhin „brav" bei solchen Servern melden oder Daten schicken, müssen ihre IP-Adressen nur noch eingesammelt werden.

SO MACHEN SIE IHREN PC BOTFREI

Mit wenigen Schritten finden Sie heraus, ob Ihr PC von Bots befallen ist: Legen Sie einfach die Stop-Bot-CD aus diesem Heft ein, und starten Sie den PC davon. Findet der DE-Cleaner tatsächlich Bots, werden sie kurzerhand gelöscht. Wie einfach das funktioniert, lesen Sie in dieser Anleitung.

1 DE-Cleaner von CD starten

FÜR PCs UND NOTEBOOKS

1 Legen Sie die CD ins Laufwerk* Ihres Computers, und starten Sie ihn neu. Die meisten PCs sind so eingestellt, dass sie automatisch von CD starten. In diesem Fall erscheint

Machen Sie dann mit Schritt 4 weiter.

2 Falls der PC statt des DE-Cleaners Windows lädt, starten Sie ihn noch einmal neu. Drücken Sie aber diesmal bei Erscheinen des schwarzen Bildschirms mehrmals nacheinander die Taste zum Einblenden des PC-Startmenüs („Bootmenü"). Je nach PC-Modell kann das die F8-Taste oder auch F12 oder Esc sein. Meistens erscheint ein entsprechender Hinweis, etwa F8 to Enter Boot Menu oder F12: Boot Menu. Sollte das nicht der Fall sein, schauen Sie im Handbuch Ihres Computers nach.

3 Im folgenden Bootmenü markieren Sie mithilfe der Pfeiltasten den Eintrag für CD-/DVD-Laufwerke, etwa CDROM, und drücken auf ↵. Falls Sie mehrere CD-/DVD-Laufwerke haben, wählen Sie in der erscheinenden Liste das passende aus, zum Beispiel

4 Kurz darauf erscheint der Startbildschirm des DE-Cleaners:

Tippen Sie auf ↵, oder warten Sie fünf Sekunden, um den DE-Cleaner zu starten. Klicken Sie dann im Fenster Nutzungs- und Haftungsbedingungen auf die Schaltfläche Akzeptieren. Wenn die Meldung Ihre Virensignaturen sind älter als 7 Tage erscheint, klicken Sie auf OK.

1 DE-Cleaner auf USB-Stift kopieren

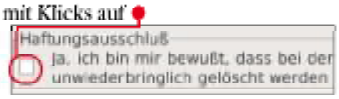
FÜR NETBOOKS

Sie benutzen ein Netbook ohne CD-/DVD-Laufwerk? Kein Problem: Der DE-Cleaner lässt sich auch komplett auf einen USB-Stift* überspielen und davon starten. Dazu genügen schon kleine Speicherstifte mit 512 Megabyte* Speicher. Weiterer Vorteil: Mithilfe des Stifts lassen sich die Bot-Informationen auch von Windows aus aktualisieren. Das Einrichten einer Internetverbindung im DE-Cleaner ist dann auch auf PCs und Notebooks nicht mehr nötig. So funktioniert die Übertragung auf den Stift:

1 Schließen Sie den externen Datenträger an, im Beispiel einen USB-Stift. Stellen Sie sicher, dass darauf keine wichtigen Daten gespeichert sind: Der Inhalt des Stifts wird bei der Installation überschrieben. Starten Sie den DE-Cleaner, und klicken Sie auf Sonstiges und auf

2 Im nächsten Fenster ist Ihr Stift bereits als Ziel-Laufwerk* ausgewählt, etwa

Falls nicht, klicken Sie auf ▼ und wählen den passenden Eintrag in der Liste. Bestätigen Sie nun mit Klicks auf



und OK, dass die Software vorhandene Dateien löscht und der DE-Cleaner auf dem USB-Speicherstift installiert wird. Wenn die Meldung Fertig! erscheint, klicken Sie auf

3 Um später den DE-Cleaner vom USB-Speicherstift zu starten, stöpseln Sie das Gerät an und schalten dann den Computer ein.

Sollte der Computer nicht automatisch vom Stift starten, befolgen Sie die Anweisungen im Abschnitt „DE-Cleaner von CD starten". Wählen Sie aber diesmal im Bootmenü den Eintrag für das Laufwerk aus, im Beispiel für Ihren USB-Speicherstift.

2 Bot-Schutz aktualisieren

FÜR PCs, NOTEBOOKS UND NETBOOKS

Die Bot-Mafia schläft nicht – jeden Tag kommen viele neue Schädlinge. Bringen Sie deshalb den Bot-Schutz vor dem Suchlauf auf den neusten Stand. Je nach Art Ihrer Internetverbindung gibt's dazu verschiedene Wege:

BOT-SCHUTZ PER KABELVERBINDUNG AKTUALISIEREN

1 Ist Ihr PC per Kabel an einen Router* angeschlossen, sind Sie in der Regel gleich nach dem Start des DE-Cleaners mit dem Internet verbunden. Probieren Sie's aus: Klicken Sie auf Sonstiges und auf das Symbol

Laden Sie im daraufhin erscheinenden Internet-Zugriffsprogramm* eine beliebige Seite. Wenn sie erscheint, steht die Verbindung. Machen Sie in diesem Fall gleich mit Schritt 3 weiter.

2 Mit einigen Netzwerkkarten (mit dem Realtek-Chip r8169) klappt die Verbindung nicht. Ist die Verbindung in Schritt 1 gescheitert, probieren Sie Folgendes: Beenden Sie den DE-Cleaner mit Klicks auf ⏻ und OK, und schalten Sie den PC wieder ein. Sobald die Startauswahl

erscheint, drücken Sie Esc. Tippen Sie dann safemode ein, und drücken Sie auf ↵. Tippen Sie einmal auf ↑, um den Eintrag

zu markieren, und auf ↵. Probieren Sie nun erneut, eine Internetseite zu öffnen.

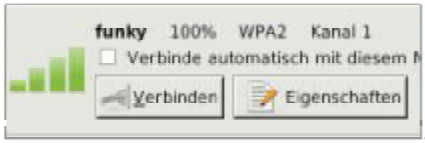
Klappt's immer noch nicht, bleibt noch die Aktualisierung über einen USB-Stift. Wie's geht, lesen Sie rechts unter dem Punkt „Bot-Schutz unter Windows aktualisieren".

3 Wenn die Internetverbindung steht, klicken Sie auf Aktualisierung und Update starten. Sobald die Meldung Update abgeschlossen erscheint, klicken Sie auf OK.

BOT-SCHUTZ PER WLAN AKTUALISIEREN

1 Falls Sie eine drahtlose Internetverbindung (WLAN*) benutzen, klicken Sie auf Sonstiges und auf

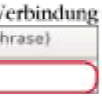
Nach wenigen Sekunden sehen Sie alle gefundenen Netzwerke*, im Beispiel



*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 132/133.

Falls die Software keine Netzwerke findet, funktioniert es bei Ihnen leider nicht per WLAN. Probieren Sie es in diesem Fall kabelgebunden, wie im Abschnitt „Bot-Schutz per Kabelverbindung aktualisieren" beschrieben.

2 Wurden Netzwerke gefunden, klicken Sie beim Eintrag der gewünschten Verbindung auf Eigenschaften, tippen hier Ihr WLAN*-Kennwort ein und klicken auf OK. Nach einem Klick auf Verbinden wird die Verbindung mit dem Internet hergestellt. Schließen Sie das Fenster per Klick auf Quit.



3 Starten Sie die Aktualisierung mit Klicks auf Aktualisierung und Update starten. Wenn die Meldung Update abgeschlossen erscheint, klicken Sie auf OK.

BOT-SCHUTZ UNTER WINDOWS AKTUALISIEREN (NUR VOM USB-STIFT)

Funktioniert die Internetverbindung im DE-Cleaner nicht, oder hätten Sie's gern bequemer? Dann übertragen Sie das System auf einen USB-Speicherstift, wie im Abschnitt „DE-Cleaner auf USB-Stift kopieren" beschrieben. Danach können Sie die Aktualisierungen von Windows aus direkt auf den Stift laden. So einfach funktioniert's:

Starten Sie Windows, und stecken Sie den Stift ein. Erscheint Welche Aktion soll durchgeführt werden?, klicken Sie doppelt auf Ordner öffnen. Andernfalls tippen Sie bei gedrückter ⊞-Taste auf E und klicken doppelt auf den Eintrag für den Stift, etwa USB (G:).

Starten Sie die Aktualisierung per Doppelklick auf avupdate, Stapelverarbeitungsdatei für ..., 1 KB.

Wenn die Meldung Avira Update erfolgreich erscheint, drücken Sie eine beliebige Taste, fahren den PC herunter, und starten dann den DE-Cleaner vom Stift. Die Bot-Suche funktioniert, wie im folgenden Abschnitt beschrieben.

3 PC von Bots befreien

FÜR PCs, NOTEBOOKS UND NETBOOKS

1 Wenn der Schutz auf dem aktuellen Stand ist, kann's losgehen: Starten Sie die Bot-Suche mit Klicks auf Virusscanner und Scanner starten. Die Software untersucht nun alle Laufwerke und repariert verseuchte Dateien dabei automatisch. Der Vorgang kann eine Weile dauern. Danach meldet der DE-Cleaner das Ergebnis, etwa Suchlauf beendet - Normales Programmende. In diesem Fall ist Ihr PC frei von Bots, und Sie können den DE-Cleaner beenden, wie in Schritt 6 beschrieben.

2 Falls Schädlinge gefunden wurden, erscheint Verdächtige Dateien oder Bootsektoren gefunden. Klicken Sie auf Protokoll ansehen/speichern. Daraufhin sehen Sie einen detaillierten Prüfbericht.

3 Infizierte Dateien, die sich nicht reparieren ließen, hat DE-Cleaner umbenannt. So können sie keinen Schaden mehr anrichten, bleiben aber auf der Festplatte – für den Fall, dass es sich um einen falschen Alarm handelt. Um diese Fälle jetzt genauer unter die Lupe zu nehmen, klicken Sie auf Bearbeiten und auf Suchen. Tippen Sie im daraufhin aufklappenden Fenster renamed ein, und klicken Sie auf Suchen. Daraufhin sehen Sie den ersten Fund, etwa

```
B  Size: 68
(media/sda1/Users/hp/Desktop/eicar.com <<<
```

Falls kein Fund erscheint, tippen Sie noch auf die Taste F3.

Die Zeile enthält den Speicherort der Datei, im Beispiel liegt sie auf der Arbeitsoberfläche*. Um sie unschädlich zu machen, hat die Software „.vir" an den Dateinamen angehängt. Windows zeigt die Datei daher so an: eicar.com.vir

4 Drücken Sie auf F3, um zum nächsten Fund zu springen. Schauen Sie sich so alle umbenannten Dateien an, und klicken Sie auf ✖. Falls ein Fehlalarm dabei war, schalten Sie den PC ab, wie in Schritt 6 beschrieben, und starten Windows. Sichern Sie dann die fälschlich umbenannte Datei, etwa auf einem USB-Stift. Trennen Sie diesen Stift vom PC, und fahren Sie den Computer herunter.

Starten Sie anschließend wieder den DE-Cleaner, und aktualisieren Sie den Bot-Schutz.

5 Klicken Sie nun auf Einstellungen, und auf Datei löschen, wenn Reparatur nicht möglich. Starten Sie dann einen neuen Suchlauf, wie in Schritt 1 beschrieben. Die gefundenen Schädlinge werden diesmal gelöscht.

6 Um den DE-Cleaner zu beenden, klicken Sie nacheinander auf und OK.

Weitere Funktionen

Der DE-Cleaner bietet neben der Suche nach Bots noch einige weitere Funktionen. Folgende Extras können Sie nach einem Mausklick auf Sonstiges aufrufen:

1 Dateimanager: Über diese Funktion haben Sie Zugriff auf Ihre Dateien und Ordner, ohne Windows zu starten. So können Sie zum Beispiel Dateien löschen, die sich im Windows-Betrieb nicht entfernen lassen.

2 Laufwerke: Hier können Sie den Lese- und Schreibzugriff für alle angeschlossenen Laufwerke verwalten.

3 Anleitung: Hier finden Sie die Anleitung für den DE-Cleaner.

4 Netzwerk und WLAN: Unter diesem Menüpunkt sind alle Netzwerkeinstellungen zusammengefasst. Hier geht's lang, um eine Internetverbindung einzurichten.

5 Webbrowser: Eine Internet-Zugriffssoftware ist ebenfalls mit an Bord. Klicken Sie auf diese Schaltfläche, um sie zu starten. So können Sie im Internet surfen, ohne Windows zu starten.

6 Nutzungsbedingungen: Hier können Sie die Nutzungsbedingungen der DE-Cleaner-CD einsehen.

7 USB-Installation: Sie können den DE-Cleaner auch auf ein externes Laufwerk übertragen. Wie das geht, steht links im Abschnitt „DE-Cleaner auf USB-Stift kopieren".

8 Systemaktualisierung: Falls Sie den DE-Cleaner auf einem externen Laufwerk betreiben, können Sie hier überprüfen, ob Verbesserungen für die Software bereitstehen. Dabei handelt es sich nicht um Infos zu neuen Bots, sondern zum Beispiel um zusätzliche Treiber*, damit der DE-Cleaner auch neuere Hardware erkennt.

9 Herunterfahren: Wenn Sie die Arbeit mit dem DE-Cleaner beendet haben, klicken Sie auf diese Schaltfläche und auf OK.