

Rootkit-Jäger

Rootkits sind heimtückisch und schwer aufzuspüren. Nur wer über ihre Eigenheiten Bescheid weiß und die richtigen Spezial-Tools einsetzt, kann sicher sein, dass sein PC sauber ist.

Windows-Rootkits sind besonders gefährlich, weil sie sich so tief im Betriebssystem verankern, dass sie praktisch unsichtbar sind. Klassische Virens Scanner haben gegen ein Rootkit keine Chance. Nur spezialisierte Tools entdecken die heimlichen Schädlinge und entfernen sie dann.

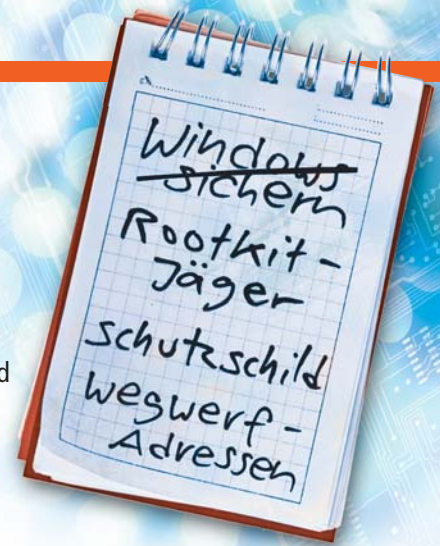
Noch vor Kurzem hatte kaum ein Antiviren-Hersteller die nötige Technik entwickelt, ein aktiviertes Rootkit zu erkennen, geschweige denn zuverlässig zu entfernen. Diese Situation hat sich mittlerweile verbessert. Einen Überblick zu den aktuellen Rootkit-Klassen und wie Sie sie entfernen, erhalten Sie

auf den folgenden Seiten. Die benötigten Tools finden Sie auf Heft-CD und -DVD sowie kostenlos im Internet.

Rootkits erkennen

Ursprünglich gab es Rootkits nur unter Unix und Linux. Doch in den vergangenen Jahren hat sich diese besonders raffinierte Schädlingsart auch unter Windows breitgemacht.

Einige Rootkits fügen Systemtreiber zu Windows hinzu oder tauschen Teile des Betriebssystems aus, so dass sie im Windows-Explorer nicht mehr angezeigt werden. Andere nisten sich im



Kompakt

- Rootkits installieren eigene Systemtreiber, damit sie unter Windows unsichtbar werden.
- Herkömmliche Virens Scanner haben kaum eine Chance, ein aktives Rootkit zu entdecken.
- Spezial-Tools und eine Rescue-CD spüren Rootkits dennoch auf.

Master Boot Record (MBR) ein oder ersetzen Anwendungen wie „explorer.exe“ durch manipulierte Versionen.

So geht s: Rootkit-Jäger Gmer 1.0.15.14972

Gmer 1.0.15.14972 (kostenlos, www.gmer.net und auf sucht nach verborgenen Prozessen, Diensten, Dateien und Registry-Einträgen auf Ihrem PC und entdeckt auf diese Weise Rootkits.

Type	Name	Value
Process	C:\Vest\hvxdef100r2\hvxdef100.exe [*** hidden ***]	1628
Service	C:\Vest\hvxdef100r2\hvxdef100.exe [*** hidden ***]	[AUTO] HackerDefender100
Service	C:\Vest\hvxdef100r\hvxdefdrv.sys [*** hidden ***]	[MANUAL] HackerDefenderDrv100

GMER
WARNING !!!
GMER has found system modification, which might have been caused by ROOTKIT activity.
Do you want to fully scan your system ?
Ja Nein

- 1 Aktives Rootkit gefunden**
Normalerweise stehen an dieser Stelle zahlreiche harmlose Einträge in schwarzer Schrift. Einträge in roter Schrift zeigen dagegen ein gefundenes Rootkit an, hier Hacker Defender.
- 2 Erweiterte Informationen**
Ein Klick auf diesen Reiter zeigt erweiterte Infos über geladene Module, aktive Dienste und die Registry.
- 3 Warning**
Gmer hat bereits beim Start ein Rootkit gefunden und weist mit diesem Warnfenster darauf hin.
- 4 Scan-Bereiche**
Hier legen Sie fest, wo Gmer überall nach Rootkits suchen soll. Am besten lassen Sie alle Kästchen angehakt.
- 5 Copy**
Ein Klick auf diesen Button kopiert den Inhalt des aktuellen Fensters in die Zwischenablage.

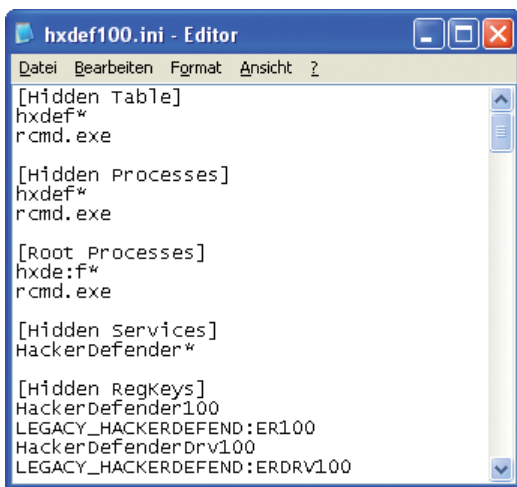
Inhalt

Windows sichern	S. 80
Rootkit-Jäger	
■ Rootkits erkennen	
Userland-Rootkits	S. 87
Kernel-Rootkits	S. 87
Application-Rootkits	S. 87
Rootkits von Firmen	S. 87
■ Rootkits bekämpfen	
Gmer 1.0.15.14972	S. 87
Avira Rescue System 3.6.9	S. 88
Rootkit-Informationen	S. 88
So geht's: Rootkit-Jäger Gmer 1.0.15.14972	S. 86
Schutzschild im Internet	S. 90
Wegwerf-Adressen	S. 92

Für die Zukunft rechnen Sicherheitsexperten mit Rootkits, die sich über die Firmware von PC-Zubehör verbreiten oder die das Betriebssystem eines PCs in eine virtuelle Kapsel verpacken. In dieser Kapsel hat dann kein Tool mehr eine Chance, das Rootkit zu entdecken.

Userland-Rootkits

Ein Userland-Rootkit fügt dem System einen Windows-Treiber hinzu, mit dem es Systemzugriffe umleitet. So macht es sich im Windows-Explorer unsichtbar. Auch beliebige Dienste, Prozesse und Registry-Schlüssel verbirgt der Schädling auf diese Weise. Selbst viele Vi-



Hacker Defender: Zu dem Rootkit gehört die Konfigurationsdatei „hxdef100.ini“. In der Regel werden hier alle Dateien und Prozesse versteckt, die mit „hxdef“ beginnen (Bild A)

rensscanner sind dagegen machtlos. Wie simpel das funktioniert, zeigt das Userland-Rootkit Hacker Defender. Das Rootkit besteht aus mehreren Dateien. Eine davon dient zum Konfigurieren der Eigenschaften des Schädlings. Der Angreifer kann hier beliebige Namen, Begriffe und Abkürzungen eingeben, die dann unter Windows nicht mehr zu sehen sind (Bild A).

Kernel-Rootkits

Ein Kernel-Rootkit tauscht Teile des Betriebssystems aus und ersetzt sie durch eigene, manipulierte Versionen. Dadurch kann es sich tarnen und beliebige Funktionen ausführen. Zu erkennen und zu entfernen sind diese Rootkits besonders schwer, da sie direkt auf Kernel-Ebene arbeiten und deswegen unbeschränkter Zugriff auf das System haben.

Application-Rootkits

Ein Application-Rootkit verbirgt sich in einem anderen Programm. Dazu wird die ausführbare Datei des Programms gegen eine manipulierte Version ausgetauscht, die den PC dann ausspioniert. Unter Windows sind Application-Rootkits noch relativ selten.

Rootkits von Firmen


Auch Firmen haben schon versucht, mit Rootkit-Techniken einen Kopierschutz durchzusetzen. Raubkopierern soll es damit schwerer gemacht werden, den DRM-Schutz (Digital Rights Management) zu entfernen.

Der bekannteste Vertreter ist das Sony-Rootkit, das sich auf mehreren Audio-CDs befand (Bild B). Der Konzern musste alle CDs zurückrufen und versprechen, Rootkits nicht mehr einzusetzen.

Rootkits bekämpfen

Rootkits sind für herkömmliche Virens Scanner unsichtbar. Zuverlässig aufspüren lassen sie sich nur mit Zusatz-Tools oder mit einem Scan, der von einer Sicherheits-CD aus gestartet wird.

Gmer 1.0.15.14972

Gmer 1.0.15.14972 (kostenlos, www.gmer.net und auf ) spürt Rootkits auf und beseitigt sie auf Wunsch auch gleich. Zudem zeigt das Tool detailliert alle Prozesse und Dienste des Systems



Sony-Rootkit: Sony hatte diese Audio-CD mit Rootkit-Technik versehen, um sie vor Raubkopierern zu schützen (Bild B)

an und hilft so bei der Suche nach verdächtigen Elementen.

So gehts: Das Anti-Rootkit-Tool benötigt keine Installation und lässt sich auch von externen Speichermedien wie USB-Sticks ausführen. Wenn Sie Gmer selbst von der Webseite des Anbieters heruntergeladen, hat das Tool immer einen anderen zufälligen Namen. So schützt es sich vor Schädlingen, die einen Wortfilter verwenden und jedes Programm mit dem Namen „gmer.exe“ blockieren. Verwenden Sie denselben Trick, falls die Gmer-Version von der Heft-CD oder -DVD auf Ihrem PC nicht starten will: Benennen Sie den ersten Teil der Datei „gmer.exe“ um und geben Sie ihr einen beliebigen anderen Namen.

Direkt nach dem Start sucht Gmer automatisch nach Rootkits. Findet es Hinweise auf ein Rootkit, so mar- ▶

kiert es diese in roter Farbe in der Ergebnisliste. Einträge in schwarzer Schrift sind harmlos und stammen vom Betriebssystem oder von installierten Anwendungen.

Je nachdem, welche Hinweise Gmer gefunden hat, müssen Sie nun anders vorgehen: Handelt es sich um einen Prozess, dann klicken Sie mit der rechten Maustaste darauf und wählen „Kill process“ aus. Ein verseuchter Windows-Dienst lässt sich mit einem Rechtsklick und „Disable service“ beenden. Weitere vorhandene Dateien eines Rootkits löschen Sie mit einem Rechtsklick darauf und der Auswahl „Delete file“.

Wenn Sie sich nicht sicher sind, welche Dateien zu einem Rootkit gehören,



Rootkit-Infos: Die englischsprachige Webseite www.rootkit.com informiert umfassend über Rootkits und bietet einige sogar zum Download an (Bild D)

Avira Rescue System 3.6.9

Prüfen Sie zusätzlich Ihren PC auch mit dem Avira Antivir Rescue System 3.6.9 (kostenlos, www.free-av.de/de/tools/12/avira_antivir_rescue_system.html und

auf). Dabei handelt es sich um eine bootfähige CD, die Ihren PC mit Antivir prüft, ohne dass Windows läuft. Das hat den großen Vorteil, dass sich ein Rootkit nicht aktivieren und verstecken kann.

So geht s: Klicken Sie doppelt auf die EXE-Datei des Antivir Rescue Systems. Es öffnet sich ein integriertes Brennprogramm, mit

dem Sie eine CD-ROM brennen. Legen Sie dazu einen CD-Rohling ein und klicken Sie auf „Brenne CD“.

Lassen Sie die CD-ROM im Laufwerk und starten Sie Ihren PC neu. Eventuell müssen Sie noch die Boot-Reihenfolge im BIOS ändern, wenn Ihr Computer nicht von der eingelegten CD startet.

Drücken Sie die Eingabetaste, sobald das Boot-Fenster des Antivir Rescue Systems erscheint (Bild C). Danach startet das Live-System. Bevor Sie anschließend Ihren PC checken, sollten Sie zuerst noch den enthaltenen Virens Scanner und die verwendeten Signaturen

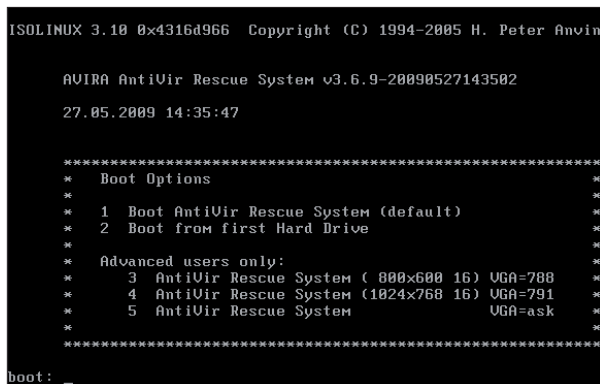
aktualisieren. Klicken Sie dazu auf „Update“ und bestätigen Sie danach mit „Ja“. Sofern eine Online-Verbindung besteht, aktualisiert das Antivir Rescue System sich nun über das Internet. Wenn Sie einen DSL-Router mit integriertem DHCP-Server verwenden, klappt die Internetverbindung automatisch. Ansonsten müssen Sie sich jeweils ein neues Antivir Rescue System von der Avira-Webseite herunterladen und auf CD brennen, um den Check immer mit einem aktuellen System durchführen zu können.

Klicken Sie nun auf „Scanner starten“, um mit der Überprüfung des Computers zu beginnen. Rechts unten sehen Sie eine Übersicht der entdeckten Schädlinge. In der Standardeinstellung protokolliert das Antivir Rescue System gefundene Schädlinge nur und löscht 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 wichtige Dateien möglicherweise unwiederbringlich gelöscht. Diese Option sollten Sie deshalb nur in Ausnahmefällen nutzen.

Rootkit-Informationen

Die englischsprachige Webseite www.rootkit.com informiert umfassend über Windows-Rootkits (Bild D). Neben Hintergrundartikeln und einem Forum finden interessierte Anwender hier sogar echte Rootkits zum Download, welche die verschiedenen Techniken demonstrieren sollen. ■

Andreas Th. Fischer
internet@com-magazin.de



Avira Rescue System 3.6.9 booten: Drücken Sie an dieser Stelle die Eingabetaste, um Ihren PC von der Reinigungs-CD zu starten (Bild C)

wenden Sie sich an ein spezialisiertes Forum. Dafür kopieren Sie die Trefferliste mit „Copy“ in die Zwischenablage und rufen www.hijackthis-forum.de oder www.trojaner-board.de auf. Erstellen Sie dort einen neuen Foreumbeitrag, in dem Sie Ihr Problem schildern und den Bericht mit [Strg V] einfügen.

Auf CD und DVD

Sie finden Gmer 1.0.15.14972 und das Avira Rescue System 3.6.9 auf in der Rubrik „Internet, Rootkit-Jäger“.

Weitere Infos

- www.diagramm.net/index.php?id=5455&d=a&i=NuN
Hintergrundinfos zu Rootkits