Spyware entlarven

„Sie kommen in Schafskleidern, inwendig aber sind sie reißende Wölfe." Dieses Bibelwort passt exakt auf die neuen Super-Viren. Wir lassen die Hightech-Tarnung auffliegen. *Von Valentin Pletzer*

In diesem Beitrag

Sie schützen Ihr System und aktualisieren es regelmäßig? Gut so. Sie glauben, dadurch sind Sie immun gegen Spyware und Trojaner? Gefährlicher Irrtum! Wer etwa auf einen Freeware-Virenscanner setzt, wiegt sich in falscher Sicherheit: Der Test in CHIP 08/07 zeigt, dass diese Programme ausgerechnet gegen die übelste Schädlings-Kategorie nichts ausrichten können: Spyware. Aber auch viele Kaufprogramme und Spezial-Tools wie Spybot Search & Destroy und Ad-Aware versagen regelmäßig im Kampf gegen moderne Schädlinge.

Wie also lässt sich Spyware aufspüren und vor allem: Wie wird man sie wieder los? Wir haben's ausprobiert und im Selbstversuch die drei meist verbreiteten Schädlinge auf unserem Test-PC installiert. Das erschreckende Ergebnis: Mit bekannten Standard-Tools lassen sie sich meist nicht entfernen. Kein Wunder, wechseln die Spione doch fast täglich ihr Gesicht, sprich Datei-Decknamen und Registry-Versteck. Selbst das Knowhow unseres mit allen Wassern gewaschenen Virenexperten half nicht weiter. „Ich krieg das Biest nicht runter", hieß es noch in der Team-Sitzung. Erst kurz vor Redaktionsschluss schaffte er es, die Spyware endgültig zu löschen - mit diesen Tricks und Tools.

SPYSHERIFF

Falsche Anti-Spyware restlos entfernen

Eine ganz perfide Spyware kommt daher wie der Wolf im Schafspelz: Getarnt als Spyware-Killer (Rogue Anti-Spyware) ver-

Illustration: QuickHoney; GettyImages

AUF CD/DVD: Die Tools finden Sie unter **CHIP-Code ⊙ ANTISPY**

leitet SpySheriff seine Opfer dazu, die Schad-Software freiwillig zu installieren. Wer darauf eingeht, bekommt den Eindringling nicht mehr los. Den dreisten Teil hebt sich das Programm bis zum Schluss auf: Bei einem vorgetäuschten Check findet der SpySheriff jede Menge Schädlinge – die gar nicht wirklich existieren. Wer die imaginären Schad-Programme loswerden will, soll zahlen – natürlich mit Kreditkarte.

Rogue Anti-Spyware aufspüren

SpySheriff erkennen Sie daran, dass er Sie mit Warnhinweisen bombardiert wie »Dieser Computer ist infiziert«. Und Sie ständig daran erinnert, jetzt die Vollversion zu kaufen. Doch das ist oft nur die Spitze des Eisbergs. Der Spion verhält sich von Fall zu Fall unterschiedlich: Mal wird nur die falsche Anti-Spyware-Komponente installiert, mal zusätzlich ein Trojaner. Nur eins ist sicher: Gegen echte Spyware unternimmt das Tool nichts!

SpySheriff entfernen

Überraschend ist die Tatsache, dass es für SpySheriff eine Deinstallations-Routine gibt. Die taucht zwar nicht im Startmenü auf, aber immerhin in der Systemsteuerung unter »Programme hinzufügen und entfernen«. Nutzen Sie die Gelegenheit und schicken Sie den SpySheriff in die Wüste – aber verlassen Sie sich nicht darauf. Wo sich die Malware auf jeden Fall immer einnistet, steht im Steckbrief rechts. Diese Einträge und Dateien lassen sich auch ganz normal mit dem Windows Explorer und dem Registry Editor entfernen.

Auf Nummer sicher gehen

In unseren Tests ließen sich verschiedene Rogue-Anti-Spyware-Programme mit dem mitgelieferten Uninstaller entfernen. Doch in einschlägigen Foren wie dem Trojaner-Board (**www.trojaner-board.de**) berichten Hilfesuchende immer wieder, dass sich noch mehr auf ihren Systemen eingenistet hat. Bei den dubiosen Geschäftspraktiken von SpySheriff und Co. lässt sich nicht ausschließen, dass die Rogue Anti-Spyware noch andere Schädlinge eingeschleppt hat. Deshalb sollten Sie sicherheitshalber die folgenden Tipps beherzigen, die wir für die anderen beiden Schädlinge anwenden, und Ihr System mit den Tools HijackThis, Autoruns und Blacklight genau unter die Lupe nehmen.

Täterprofil

Name
SpySheriff

Charakteristik
tarnt sich als Virenscanner

Alias
Adware Sheriff, SpyAxe, SpywareQuake

Aktive Prozesse
1950.exe, newdial.exe, spysheriff.exe, uninstall.exe, winstall.exe

Registry-Verstecke
HKLM\SOFTWARE\spysheriff,
HKLM\SOFTWARE\Microsoft\Windows\,
CurrentVersion\uninstall\spysheriff

Datei-Decknamen
%ProgramFiles%\spysheriff,
1950.exe, Desktop.html, newdial.exe,
spysheriff.exe, uninstall.exe,
winstall.exe,
%UserProfile%\Desktop\SpySheriff.lnk

Gefährliche Täuschung

Hinter der scheinbar harmlosen Website verbirgt sich eines der nervigsten Schadprogramme: SpySheriff.

Ein professionelles Logo und eine schicke Packung lassen die Malware ganz seriös erscheinen.

Hinter dem Button »Free Scan« verbirgt sich kein kostenloser Virencheck, sondern die EXE der SpySheriff-Spyware, die Ihren Rechner infiziert.

Die Produkt-Beschreibung liest sich wie die eines echten Spyware-Killers. Wer das Programm nicht kennt, fällt leicht darauf rein.

VUNDO

Agressive Hijacker endgültig loswerden

Der Schädling, den wir uns als nächstes vorknöpfen, ist mit Abstand der agressivste. Mit dem Ziel, unseren Testrechner zu verseuchen, suchen wir auf Google nach einer gehackten Seriennummer. Denn in solchen verlockenden, aber illegalen Angeboten verstecken sich besonders oft Hijacker und Downloader. Zwar warnt uns Google vor der möglicherweise schädlichen Webseite, doch wir ignorieren das und öffnen sie.

Dann geht alles ganz schnell: Die Seite baut sich auf, die Schadroutine wird aktiv, der PC ist verseucht. Vundo heißt der Schädling – ein Downloader. Doch das erfahren wir erst später, als wir eine verdächtige Datei von 18 verschiedenen Virenscannern prüfen lassen. Nur eine Handvoll davon erkennt den Downloader →

Täterprofil

Name
Vundo

Charakteristik
greift Virenscanner an

Typ
Hijacker, Downloader und Trojaner

Prozesse
zwei jedes Mal zufällig erzeugte DLLs

Registry-Verstecke
HCR\clsid\{EFCB1D95-FFF6-47BB-B6C9-61A523F04322},
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

Festplatten-Versteck
C:\Windows\System32\

überhaupt. Und wie der Gattungsname schon sagt, beginnt der Eindringling sofort damit, andere Schad-Software nachzuladen. In unserem Fall ein Plugin für den Internet Explorer, das uns mit Werbe-Popups aller Art bombardiert.

Um den Schädling zu vernichten, installieren wir die Freeware Ad-Aware 2007. Die erkennt Vundo zwar – kann den Downloader aber nicht vollständig löschen. Nach jedem Neustart ist er wieder da. Noch weniger Erfolg haben wir mit Spybot Search & Destroy: Wir starten das Setup, können es aber nicht abschließen. Vundo killt immer wieder den Prozess und verhindert damit eine erfolgreiche Installation des Spyware-Killers. Schwereres Geschütz ist also notwendig, um der Plage Herr zu werden.

Schad-Software erkennen

Solange auch nur ein Prozess der Schad-Software aktiv ist, kriegt man sie nicht mehr vom System. Deshalb muss zuerst die Malware und alle ihre Verstecke identifiziert werden. Installieren Sie dazu das Tool Autoruns (kostenloser Download unter **www.sysinternals.com**).

Die Freeware erledigt im Prinzip den gleichen Job wie das unter Spyware-Jägern beliebte Programm HijackThis. Im Gegensatz dazu listet es jedoch sämtliche Autostart-Einträge in der Registry auf. Denn anders als noch vor einigen Jahren, trägt sich die Malware nicht mehr nur unter „Run“ oder „RunOnce“ ein. Beispiel Vundo: Dieser Eindringling nistet sich gleich noch an drei anderen Stellen ein.

Um die zu lokalisieren, öffnen Sie Autoruns und setzen als erstes ein Häkchen bei »Verify Code Signatures« und »Hide Microsoft Entries«. Der Hintergrund: Jede ausführbare Datei kann vom Ersteller mit einem Namen und einer digitalen Signatur versehen werden. Bei jeder Original-Microsoft-Datei ist das zum Beispiel der Fall. Mit den genannten Einstellungen filtern Sie diese Dateien heraus und sparen sich eine Menge Recherche-Arbeit.

Die restlichen Dateien müssen Sie manuell verifizieren. Auch dabei hilft Autoruns. Wählen Sie einen Eintrag mit der rechten Maustaste aus und klicken Sie auf »Search online ...«. Dann wird der Dateiname mit Microsofts Suchmaschine Live.com gesucht. In einigen Fällen lassen sich so die Dateien von bekannten Schädlingen identifizieren. Übrig bleibt eine Liste von suspekten Dateien und Registry-Einträgen, die Sie löschen sollten.

Schädlinge abschalten

Leider ist Vundo so agressiv, dass es nicht reicht, die Registry-Einträge zu entfernen. Denn die aktiven Komponenten des Eindringlings restaurieren die Einträge einfach wieder. Hier hilft jedoch ein Trick: Laden Sie den Process Explorer von **www.sysinternals.com** herunter und starten Sie das Tool. Nach einem kurzen Scan zeigt es sämtliche aktiven Prozesse an. Der Trick besteht nun darin, die Hijacker-Dateien nicht aus dem Speicher zu löschen, sondern erst einmal nur zu deaktivieren. Klicken Sie dazu mit der rechten Maustaste auf den verdächtigen Prozess und wählen Sie »Suspend« aus. Damit lähmen Sie den Prozess nur – die Prüfroutine der anderen Hijacker-Prozesse merkt davon nichts. Jetzt haben Sie es fast geschafft.

Hijacker löschen

Ist der Angreifer dank dem Process Explorer lahm gelegt, lässt er sich bequem entfernen. Notieren Sie sich zuerst Namen und Pfad all jener Dateien, die Sie dem Eindringling zuordnen konnten. Beenden

Diese Tools entfernen jede Spyware

Hat sich die Malware erst einmal festgesetzt, bekommt man sie nur mit den richtigen Tools wieder los. Die Besten haben wir für Sie unter dem CHIP-Code ANTI-SPY zusammengestellt.

HijackThis 2.0.2 ○ ○
Browser-Hijacker lassen sich besonders gut mit diesem Tool finden und entfernen. Aber nur, wenn man die Stärken und Schwächen des Programms kennt.
www.hijackthis.de

Autoruns 8.7 @
Dieses Profi-Tool kennt alle Registry-Verstecke, die sich als Autostart-Plattform nutzen lassen. Wenn Sie eine Malware im System vermuten, stehen die Chancen gut, dass Sie sie hier finden und am Starten hindern können.
www.sysinternals.com

Process Explorer 10.21 @
Um Spyware-Prozesse zu finden und zu killen, reicht das Windows-Boardmittel Taskmanager nicht aus. Der Process Explorer löst dieses Problem und bietet zudem noch mehr Funktionen.
www.sysinternals.com

Pocket KillBox 2.0 ○ ○
Die Methoden der Spyware werden immer rabiater. Beenden Sie einen Prozess, startet ihn ein anderer erneut. Die KillBox macht endgültig Schluss damit.
www.killbox.net

F-Secure BlackLight 2.2.1055 B. ○ ○
Immer öfter versteckt sich Malware mit Hilfe von Rootkit-Techniken. Dieses Tool von F-Secure macht die Schädlinge wieder sichtbar – zumindest die meisten.
www.f-secure.de

Gmer 1.0.13 ○ ○
Ein Anti-Rootkit reicht für die Analyse nicht. Denn nicht jedes Tool kennt alle Tricks. Als Ergänzung zu BlackLight eignet sich diese Software besonders gut.
www.gmer.net

virusscan.jotti.org
Verdächtige Dateien sollten auf jeden Fall von einem Virenscanner gecheckt werden. Jordi Bosveld bietet eine kostenlose Webseite an, die gleich mit 15 verschiedenen Virenscannern prüft.
http://virusscan.jotti.org

○ auf Heft-CD ○ auf Heft-DVD @ Link auf CD/DVD

Sie dann mit dem Process Explorer per »Kill«-Befehl alle Prozesse, die Sie zuvor mit dem »Suspend«-Befehl zum Schlafen geschickt haben.

Als nächstes löschen Sie mit Autoruns sämtliche Einträge, die Sie identifizieren konnten. Klicken Sie dazu mit der rechten Maustaste auf den verdächtigen Eintrag und wählen Sie »Delete«. Jetzt ist die Gefahr fast gebannt. Löschen Sie in einem finalen Schritt noch die gefährlichen Dateien, damit sie nicht aus Versehen aufgerufen werden. Nach einem Neustart sollte Windows wieder frei von Schädlingen sein. Jetzt funktionieren auch Spybot Search & Destroy und Ad-Aware wieder. Überprüfen Sie mit diesen Tools noch, ob Sie wirklich nichts übersehen haben.

ZLOB

Gefährliche Video-Codecs sicher entfernen

Mit Sprüchen wie „Paris Hilton nackt“ und „Alle Blockbuster kostenlos“ locken Webseiten, die nur ein Ziel haben: Den PC des Users unter Kontrolle zu bekommen. Der Trick: Wer einen so beworbenen Film abspielen möchte, muss den ebenfalls beworbenen Codec installieren – und hat dann die Malware Zlob im Gepäck.

Zu Testzwecken gehen wir auf das falsche Spiel ein und werden prompt infiziert. Angegriffen fühlen wir uns erst einmal nicht, denn der falsche Codec hat sogar einen offiziellen Uninstaller. Das ist natürlich geschwindelt: Ganz entfernen lässt sich Zlob damit nicht.

Schädling enttarnen

Ein erster Hinweis darauf, dass etwas faul ist, geben die Netzwerk-Einstellungen. Typischerweise werden in einem Heimnetzwerk die Name-Server vom DHCP-Server verteilt. Das heißt, der DSL-Router kümmert sich um die Adressvergabe, und am Windows-Rechner ist diese Option eingestellt: »DNS-Serveradresse automatisch beziehen«. Der falsche Codec installiert nun einen DNS-Changer-Trojaner, der eigene Server aktiviert. Einmal eingestellt, kann der Betreiber des Servers jeden Schritt des Opfers im Netz nachvollziehen und sogar umlenken. Diese Modifikation wird von Tools wie Spybot Search & Destroy erkannt und repariert. Doch die Ursache des Ganzen, das Rootkit, bleibt aktiv. So ist nach einem Neustart alles beim Alten – also beim Schlechten.

Täterprofil

Name
Zlob

Charakteristik
versteckt sich in Rootkits

Alias
DvdCodec, UseCodec, KeyCodec, EliteCodec, PerfectCodec, PornMagPass, QualityCodec, VCCodec, XPassword Generator, ZCodec, ZipCodec

Prozesse
kd*.exe

Registry-Versteck
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\System

Festplatten-Verstecke
C:\Windows\System32\kd*.exe,
C:\Programme\PornoPlayer*.*

Sonstiges
verändert die Einstellungen des DNS-Servers im Netzwerk

Rootkit sichtbar machen

Um sich gegen Zugriffe zu schützen, greift der DNS-Changer-Trojaner zu einem besonders fiesen Trick: Jede Anfrage an das Dateisystem wird nicht direkt vom Betriebssystem beantwortet, sondern erst durch ein Rootkit manipuliert. Sicherheits-Programme bekommen den Trojaner gar nicht zu Gesicht, weil er sich ganz einfach selbst aus der Liste streicht. Und genau daran scheitern Spybot Search & Destroy, Ad-Aware und andere Anti-Spyware. Abhilfe schafft nur ein Anti-Rootkit-Tool. Doch leider auch nicht jedes. So wird der Eindringling nicht von Sysinternals' Rootkit Revealer erkannt. Blacklight von F-Secure hingegen schafft das. Scannen Sie damit Ihr System, so findet das Tool eine EXE-Datei, die sich aus „kd“ und drei weiteren, zufällig gewählten Buchstaben zusammensetzt.

Schadcode löschen

Das Programm von F-Secure bietet eine Option zum Löschen. Wählen Sie diese und starten Sie danach den PC unbedingt neu. Sonst ist der Trojaner noch im Speicher aktiv und kann sich im schlimmsten Fall selbst wiederherstellen. Nach dem Neustart sollten Sie dringend noch den Winlogon-Registry-Eintrag (siehe Täterprofil) entfernen. Öffnen Sie dazu Autoruns und anschließend den Reiter »Logon«. Hier steht der Eintrag, den Sie mit einem rechten Mausklick und »Delete« löschen sollten. Sonst kann es passieren, dass eine gleichnamige Datei aus dem „System32“-Verzeichnis beim nächsten Systemstart mitgeladen wird.

Eventuelle Malware-Reste lassen sich wieder mit Spybot Search & Destroy oder Ad-Aware entfernen. Dann hat der Spuk wirklich ein Ende! *valentin.pletzer@chip.de*