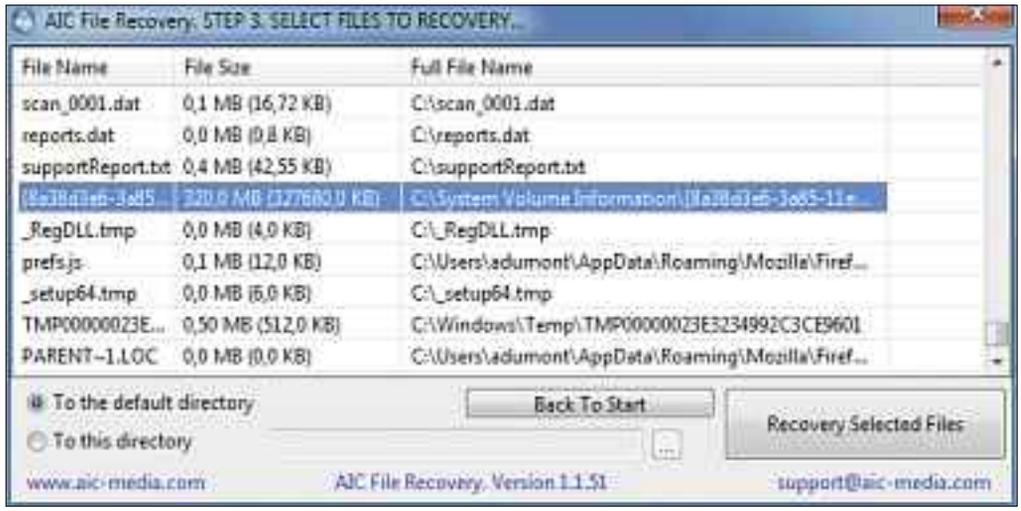
AIC FILE RECOVERY 1.1.51

Dateien retten

Versehentlich gelöschte Dateien lassen sich mit AIC File Recovery 1.1.51 wieder rekonstruieren (kostenlos, www.aic-media.com/products/filerecovery und auf).

Installieren und starten Sie das Tool. Wählen Sie dann die Partition aus, auf der Sie Dateien wiederherstellen wollen. Klicken Sie zunächst auf "Find Deleted Files", um den Suchlauf zu starten. Markieren Sie dann die zu rettenden Daten und bestätigen Sie mit einem Klick auf den Button "Recovery Selected Files" (Bild A).

Hinweis: Das Programm benötigt Administratorrechte, um gelöschte Daten wiederherstellen zu können.



AIC File Recovery 1.1.51: Das Tool sucht nach gelöschten Dateien und stellt diese wieder her (Bild A)

OB-PWD 0.54

Sichere Passwörter

Eine Firefox-Erweiterung erzeugt auf eine neuartige Art und Weise komplizierte, unknackbare Passwörter (Bild B).

Ob-Pwd 0.54 erzeugt Passwörter aus Bildern, ganz gleich ob diese online sind oder sich auf dem PC befinden (kostenlos, https://addons.mozilla.org/en-US/firefox/addon/obpwd-object-based-password-pa und auf).

Ob-Pwd steht für Object-based Password. Das Tool nutzt dabei die ersten 100'000 Bytes des Objekts, um das Passwort zu generieren.

Anschliessend lassen sich die Passwörter per Kopieren und Einfügen in die entsprechenden Felder übertragen. Sie müssen sich das komplizierte Passwort nicht merken, sondern nur, mit welchem Bild Sie es erzeugt haben. Die Standardlänge des generierten Passworts ist zwölf Zeichen, lässt sich aber in den Einstellungen der Erweiterung anpassen.

PROXY TOOL 1.16

User Agent String verbergen

Der User Agent String verrät, mit welchem Browser und mit welchem Betriebssystem Sie unterwegs sind. Eine Firefox-Erweiterung verschleiert diese Informationen.

Ein typischer User Agent String lautet beispielsweise "Mozilla/5.0 (Windows NT 6.1; U; WOW64; de; rv:2.0b11) Gecko/20100101 Firefox/4.0b11".

Dieser Nutzer surft mit dem Browser Firefox 4.0 Beta 11 auf dem Betriebssystem Windows 7 64 Bit. Ausserdem kommt er aus Deutschland und hat den Sicherheitsstandard U – das steht für sicher. Auch das Build-Date des Browsers geht daraus hervor. Im Beispiel-String ist es der 1. Januar 2010.

All dies sind wertvolle Informationen für einen potenziellen Angreifer. Einen Schutz bietet die Firefox-Erweiterung Proxy Tool 1.16 (kostenlos, https://addons.mozilla.org/de/firefox/addon/proxytool und auf).

Nach der Installation klicken Sie mit der rechten Maustaste auf eine beliebige Stelle im Browserfenster und wählen aus dem Kontextmenü den Punkt "User Agent, Zufällig (Alle)". Proxy Tool zeigt daraufhin für jede Webseite wechselnde, zufällige User Agent Strings an, die keine Rückschlüsse auf Ihren Browser oder Ihr Betriebssystem ermöglichen.

Um Ihren User Agent String auszulesen, rufen Sie die englischsprachige Website www.useragentstring.com auf.

FIREFOX 4

Tracking-Schutz aktivieren

Firefox 4 enthält die neue Funktion "Do Not Track". Sie soll davor schützen, dass Seitenbetreiber Nutzerprofile erstellen, ist aber standardmässig deaktiviert.

Damit können Nutzer Webseiten mitteilen, dass sie kein Tracking durch Werbenetzwerke wünschen. Das erfolgt über einen speziellen HTTP-Header. Was der Anbieter damit macht, bleibt ihm überlassen, so dass der Ansatz keinen direkten Schutz bietet. Die Aktivierung kann gleichwohl nicht schaden.

Um die Funktion einzuschalten, gehen Sie über den Firefox-Button zu den "Einstellungen". Dort klicken Sie auf "Erweitert" und wechseln zum Reiter "Allgemein". Hier setzen

Sicherheits-Tipp des Monats: Spyware aufspüren

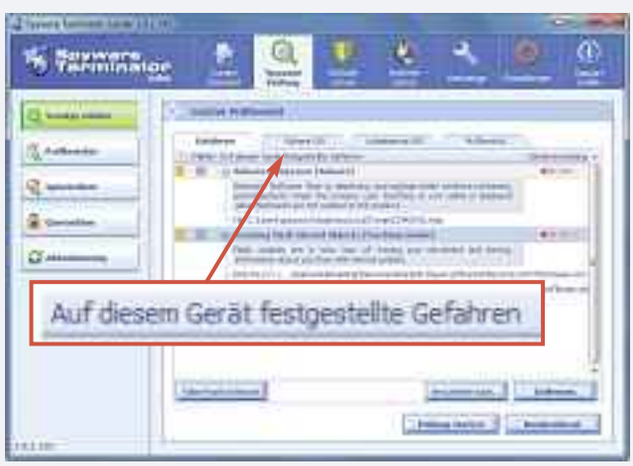
Spyware kompromittiert Ihre Privatsphäre und gefährdet die Sicherheit Ihres Systems. Ein kostenloses Tool scannt Ihren PC und beseitigt Schnüffelsoftware.

Spyware Terminator 2.8.2.192 ist auf Spyware spezialisiert, spürt jedoch auch andere Malware auf (kostenlos, www.spywareterminator.com/de).

Das Programm bringt einen Echtzeitschutz mit und eine automatische Update-Funktion für die Datenbank.

Nach dem Start wechseln Sie zu "Spyware Prüfung". Dort wählen Sie den gewünschten Scan-Typ aus und starten die Suche mit einem Klick auf "Prüfung starten". Anschliessend erhalten Sie eine Liste der aufgespürten Spyware. Sie haben die Möglichkeit, diese einzeln oder in einem Rutsch zu löschen (Bild C).

Hinweis: Während der Installation versucht Spyware Terminator, die Toolbar Web Security Guard zu installieren. Diese ist unnötig.



Spyware Terminator 2.8.2.192: Das Programm durchkämmt Ihr System nach Ad- und Spyware und löscht sie (Bild C)

Auf DVD

Sie finden AIC File Recovery 1.1.51, Ob-Pwd 0.54 und Proxy Tool 1.16 auf in der Rubrik "Computer, Sicherheits-Tipps".

Sie ein Häkchen bei "Websites mitteilen, dass ich nicht verfolgt werden möchte".

WINDOWS XP

Hosts-Datei schützen

Die Hosts-Datei legt fest, welche Webseite der Browser tatsächlich lädt, wenn Sie eine URL eintippen. Schützen Sie die Hosts-Datei, damit Sie nicht auf gefälschte Webseiten umgelenkt werden.

Unter Windows Vista und 7 lässt sich die Hosts-Datei nur mit Administratorrechten ändern und ist somit bereits gut geschützt. Bei Windows XP müssen Sie selbst Hand anlegen. Navigieren Sie im Windows-Explorer zum Ordner "C:\WINDOWS\system32\drivers\etc". Klicken Sie mit der rechten Maustaste auf die Datei "hosts". Wählen Sie dann im Kontextmenü den Punkt "Eigenschaften" aus und setzen Sie bei den Attributen ein Häkchen vor "Schreibgeschützt".

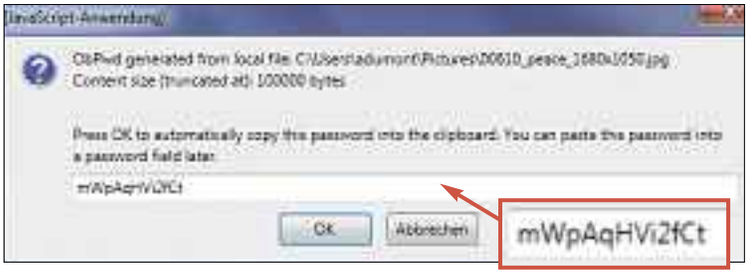
ROGUE ANTI-SPYWARE

Falsche Schutzprogramme

Falsche Sicherheitsprogramme geben vor, Hunderte Viren auf Ihrem Rechner gefunden zu haben, und bieten an, diese gegen Gebühr zu entfernen (Bild D). Solche Programme lassen sich bereits im Vorfeld erkennen.

Bevor Sie ein unbekanntes Schutzprogramm installieren, suchen Sie auf der Seite http://rogueantispyware.blogspot.com danach. Wenn Sie dort fündig werden, dann lassen Sie besser die Finger von dem Programm.

Auch wenn Sie ein solches betrügerisches Programm bereits auf Ihrem System haben, ist die Seite eine gute Anlaufstelle. Sie enthält detaillierte Anleitungen, wie Sie dieses wieder loswerden – allerdings auf Englisch.



Ob-Pwd 0.54: Die Firefox-Erweiterung erzeugt aus Bildern sichere Passwörter (Bild B)

WINDOWS XP, VISTA UND 7

Microsoft Security Essentials gefälscht

Eine Fälschung des Sicherheitsprogramms Microsoft Security Essentials (MSE) tut zunächst so, als ob es einen Virus beseitigt. Dann empfiehlt das Fake-MSE gegen eine vermeintliche Lücke im Dateisystem das Tool Windows Express Settings. Dieses Programm checkt den Rechner angeblich und "findet" gleich eine ganze Reihe von Schädlingen. Um diese zu entfernen, soll man 80 Dollar für eine Lizenz zahlen – per Kreditkarte.

http://viruslab.blog.avg.com/2011/02

Windows Optimal Settings: Dieses Programm ist eine Fälschung, die nur auf Ihr Geld aus ist (Bild D)

AUTORUN REAKTIVIEREN

Fix it für Autorun

Mit Patch 967940 für XP und Vista hat Microsoft kürzlich die Autorun-Funktion für USB-Sticks ausgeschaltet. Damit wird verhindert, dass sich beim Einstecken des USB-Sticks automatisch ein Fenster öffnet. Nun gibt es ein Fix-it-Tool, mit dem man die Funktion reaktivieren kann.

http://support.microsoft.com/kb/967715/en-us

SPASS- UND SCHOCKVIDEOS

Likejacking-Angriff gegen Facebook

Kriminelle missbrauchen vermehrt den "Gefällt mir"-Button von Facebook. Beim Likejacking locken sie mit spektakulären Videos etwa vom Tsunami in Japan oder vom angeblich toten Charlie Sheen. Hinter dem Video liegt ein unsichtbarer Rahmen mit dem "Gefällt mir"-Button. Wer daraufklickt und gerade bei Facebook eingeloggt ist, verbreitet ohne es zu merken Werbung für das Video auf der Pinnwand seiner Facebook-Kontakte und läuft Gefahr, seinen PC mit Schadsoftware zu infizieren.

http://nakedsecurity.sophos.com/2011/03/13 ■

Andreas Dumont/jb