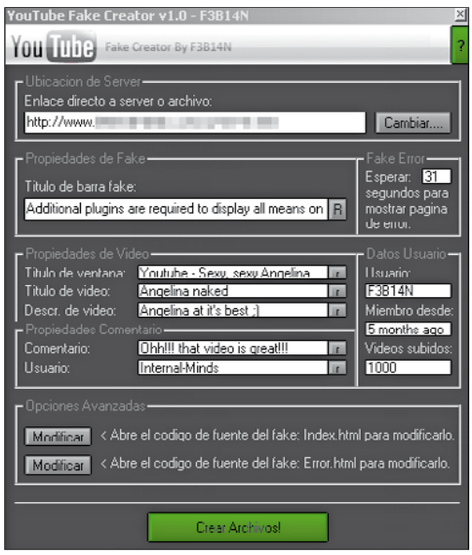
Computer Bild Sicherheits-Center

BASTELBOX FÜR VIREN

Die meisten Schadprogramme entern den PC über infizierte Internetseiten. Eine neue Hacker-Software, die verseuchte Seiten erstellt, könnte diese Gefahr nun deutlich erhöhen.

Witziges, Haarsträubendes, Sport, Musik und Erotik: Es gibt kaum etwas, worüber sich bei YouTube kein Video findet. Doch die Beliebtheit des weltweit größten Online-Filmportals nutzen jetzt Cyber-Kriminelle, um im großen Stil Schadprogramme über das Internet zu verbreiten.

Hacker haben eine gefährliche Software ins Internet gestellt, mit der selbst Anfänger ohne Programmierkenntnisse YouTube-Seiten fälschen und mit Schadprogrammen verseuchen können. Das Programm heißt YouTube Fake Creator und wird über geheime Hacker-Seiten im ausgetauscht.



Mit YouTube Fake Creator lassen sich virenverseuchte YouTube-Seiten bauen. Die spanischsprachige Software bieten Hacker im Internet an.

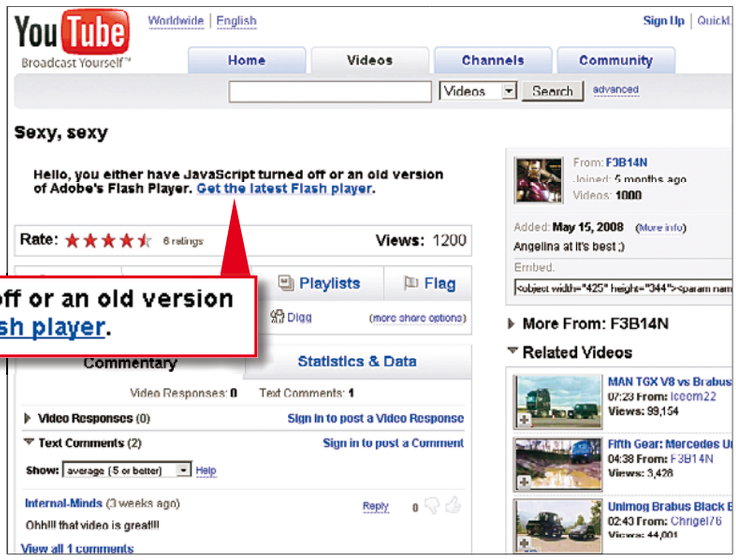
Viren-Baukasten für Anfänger

Panda Software, Hersteller von Viren-Schutzprogrammen, hatte als Erster vor der neuen spanischsprachigen Schädlingssoftware gewarnt. Die Sicherheitsexperten von COMPUTERBILD untersuchten YouTube Fake Creator, und das Ergebnis lässt wenig Gutes ahnen:

Hello, you either have JavaScript turned off or an old version of Adobe's Flash Player. Get the latest Flash player.

Mit dem Baukasten lassen sich tatsächlich mit ein paar Klicks täuschend echte, englischsprachige YouTube-Seiten zusammenbasteln (siehe Bild rechts) und darüber Schadprogramme verbreiten. Es genügt, im Viren*-Baukasten eine Filmkategorie zu wählen, die bei YouTube-Besuchern besonders beliebt ist – etwa erotische Filme. Im Beispiel (Bild links) werden potenzielle Opfer mit dem Versprechen auf ein schlüpfriges Video mit Angelina Jolie geködert.

Die mit Fake Creator erstellten Seiten speichert der Seitenfälscher einfach auf irgendeinem Computer im Internet. Die Internetadresse der Fake-Seite verteilt er dann massenhaft über interessant klingende Spam-Mails.



Die von COMPUTERBILD zum Testen erstellte YouTube-Seite ist vom Original nicht zu unterscheiden. Wer so eine Seite öffnet, um den Film anzusehen, soll den neuesten Flash Player installieren. Doch statt des Flash Players werden Viren überspielt.

Der Trick, mit dem Schadprogramme anschließend auf fremde PCs gelangen: Beim Starten der gefälschten Seite wird kein Video abgespielt. Die vorgeschobene Begründung: Der Nutzer soll erst das Video-Abspielprogramm Flash Player aktualisieren. Doch statt der neuen Player-Version bekommt er ein Schadprogramm auf den Computer.

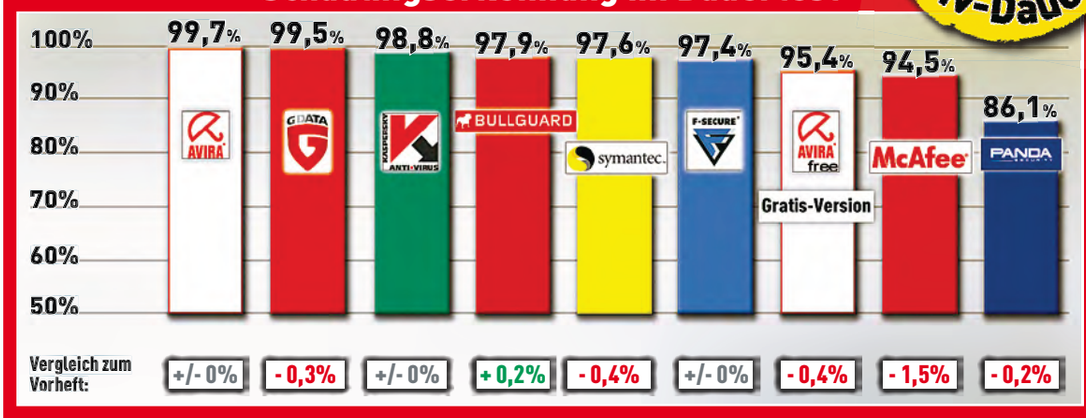
Mit dem Viren-Baukasten können die Hacker jeden beliebigen Schädling verbreiten, der ihnen zur Verfügung steht, etwa Trojaner*, mit denen sich private Infos von infizierten Computern schleusen lassen. Der beste Schutz gegen solche Tricks sind ein ständig aktualisiertes Internet-Schutzpaket mit Spam-Filter und große Skepsis bei fremden E-Mails mit zwielichtigen Angeboten. *[opu]*

SCHUTZ VOR FAKE-SEITEN

- Klicken Sie nicht auf Internetverweise, die in offensichtlichen Spam-Mails stecken.
- Wenn Sie eine Software aktualisieren müssen, starten Sie den Überspielvorgang nicht von irgendeiner Internetseite. Nutzen Sie dafür besser die Aktualisierungsfunktion der Software oder eine vertrauenswürdige Internetseite – entweder die des Programmherstellers oder von computerbild.de.

Computer Bild Woche 38/08 Exklusiv-Dauertest

Schädlingserkennung im Dauertest



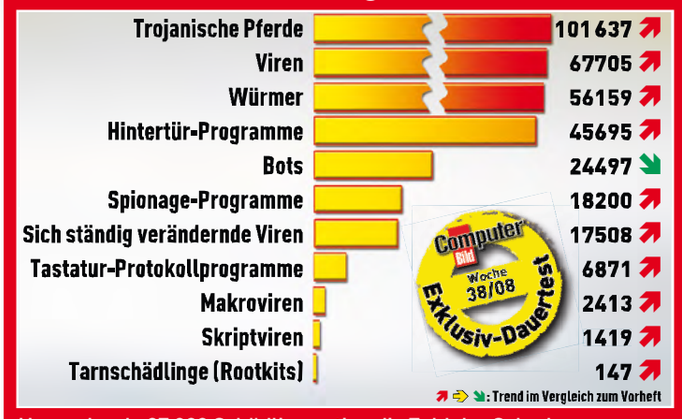
Deutliche Veränderungen in der Rangliste der Sicherheitspakete: Das Schutzprogramm von Avira stößt den bisherigen Spitzenreiter vom Thron. Denn die Erkennungsrate des Sicherheitspakets von G Data ist gesunken. Verbessern konnte sich nur ein Programm: Die Software von Bullguard, die damit den Platz mit dem Symantec-Programm tauscht. Die größten Anpassungsschwierigkeiten an die aktuelle Bedrohungslage zeigt McAfee: minus 1,5 Prozent Erkennungsleistung.

DER TEST IN ZAHLEN

- **35 000** Schädlinge täglich erfassen die Viren-Experten von AV-Test in Magdeburg im Auftrag von COMPUTERBILD in exakten Messungen – die größte aktuelle Virensammlung weltweit!
- **150** Computer sammeln dafür rund um die Uhr Viren im Internet.
- **1 MILLION** neuer Viren prüft COMPUTERBILD ständig in sekundengenauen Messungen darauf, wie sie auf den Computer gelangen und sich verbreiten.
- **260 000** aktuelle Schädlinge pro Woche müssen die Sicherheitspakete erkennen.

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 170/171.

Aktive Schädlinge der Woche



Um mehr als 27 000 Schädlinge stieg die Zahl der Schadprogramme auf nun 342 251. Nach wie vor ist die Gefahr am größten, den PC mit einem Trojaner zu infizieren. Aber auch Viren, Hintertür- und Spionage-Programme legten stark zu. Gleichzeitig sank die Erkennungsleistung vieler Sicherheitspakete (siehe Grafik auf Seite 26).

1-2-3-KLICK-HILFE: SCHUTZ PRIVATER DATEN BEI XING

Zu wem haben Sie Kontakt aufgenommen und für welche Diskussionsgruppen interessieren Sie sich? Auf der Internetplattform Xing →① sind viele Infos für andere automatisch abrufbar, die Sie eventuell gar nicht preisgeben wollen. Aber das Portal bietet Möglichkeiten, die Privatsphäre zu schützen und solche Infos zu blocken:

1 Nachdem Sie sich bei Xing angemeldet haben, klicken Sie auf Einstellungen. Um festzulegen, wer auf Ihre Daten zugreifen darf, wählen Sie Meine Privatsphäre.

2 Nun sehen Sie, welche Ihrer Daten bei Xing von anderen einzusehen sind. Freigegebene Daten sind mit einem Haken gekennzeichnet: ☑. Gesperrte Daten erkennen Sie am Kreuz ☒.

3 Wollen Sie Daten von der Freigabeliste streichen, wählen Sie Bearbeiten und entfernen das entsprechende Häkchen. Danach bestätigen Sie mit

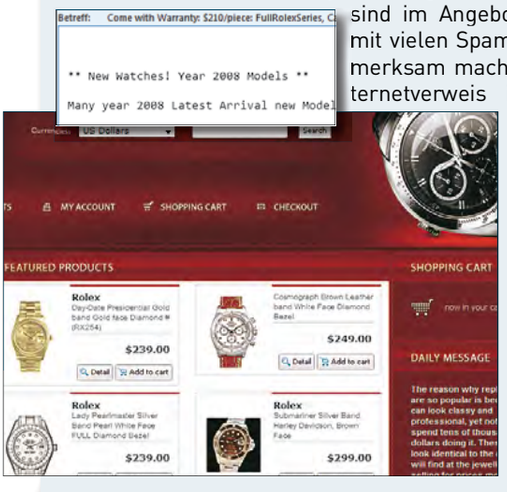
Speichern.

Nun erscheint vor Ihren gesperrten Daten ☒. Überlegen Sie genau, für wen Sie Ihre Daten verfügbar machen.

→① **www.xing.com**

+++SPAM DER WOCHE+++

Rolex, Cartier und Chopard – alle ab 210 Dollar pro Stück und mit Garantie! Wer sich mit Nobeluhren auskennt, wird eine solche E-Mail sofort richtig einschätzen. Eine neue Rolex für 210 Dollar kann nur eines bedeuten: eine Fälschung. Und davon bietet der Internetshop Greatwatchs.com jede Menge. Über 385 Chronografen sind im Angebot der Fälscher, die mit vielen Spam-Mails auf sich aufmerksam machen. Wer auf den Internetverweis in der Spam-Mail klickt, fängt sich zwar kein Schadprogramm auf dem Computer ein, doch der Kauf von Fälschungen kann teuer werden. Zum Beispiel wenn der Zoll die Uhr herausfischt und beschlagnahmt. Denn dann segnet auf jeden Fall Ihr Geld das Zeitliche.



Hier stand im Heft eine Anzeige.