Tipps zu Virustotal

Virustotal scannt Dateien nicht nur mit mehr als 40 Virenscannern, sondern prüft auch Prozesse, sucht nach Hashes und scannt Webseiten – man muss nur wissen wie.

Der kostenlose Online-Dienst Virustotal prüft Dateien mit mehr als 40 Virenscannern. Die Chance, auf diese Weise zum Beispiel in einer gerade aus dem Internet heruntergeladenen Datei einen Virus aufzuspüren, ist groß – deutlich größer, als würden Sie sich nur auf den auf dem PC installierten Virenscanner verlassen.

Virustotal nutzen

Die wichtigste Funktion von Virustotal ist der Scan einzelner Dateien mit Dutzenden von Virenscannern. Wie das geht und wie Sie das Ergebnis interpretieren, das lesen Sie im Folgenden.

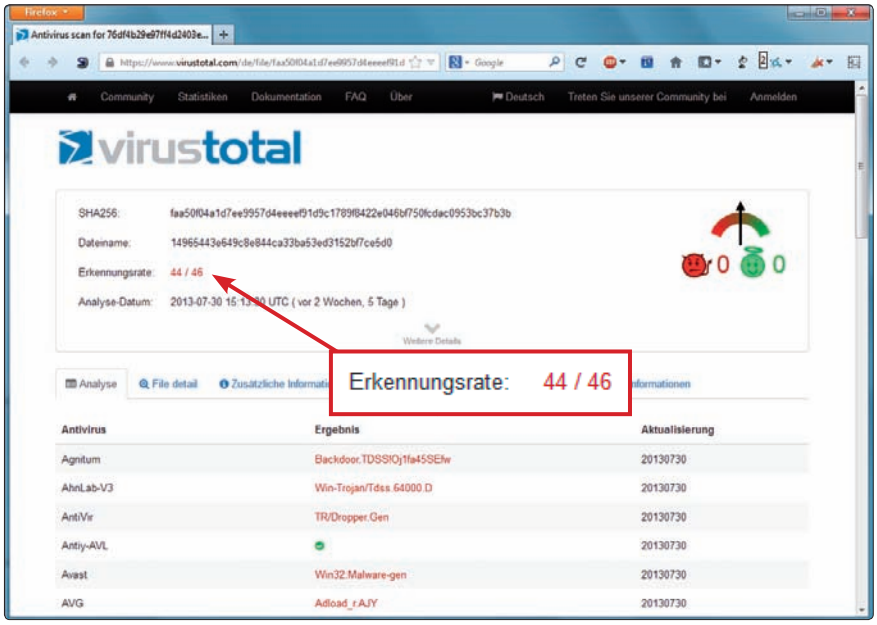
„10 Tipps zu Virustotal" zeigen dann, was Virustotal außerdem noch leistet.

Datei hochladen

Virustotal ist leicht zu bedienen: Rufen Sie die Seite www.virustotal.com/de auf und klicken Sie auf die Schaltfläche „Wählen Sie eine". Es öffnet sich ein „Datei hochladen"-Dialog. Navigieren Sie zu der Datei, die Sie prüfen lassen möchten, und klicken Sie doppelt darauf. Zurück im Browserfenster klicken Sie dann auf „Scannen!".

Bei Dateien, die Virustotal unbekannt sind, öffnet sich sofort das Analysefenster, in dem nach und nach die einzelnen Ergebnisse des Viren-Checks angezeigt werden.

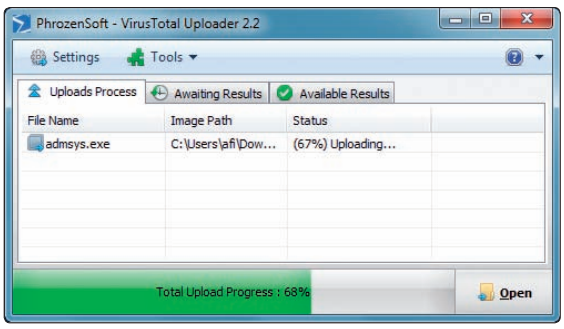
Wenn bereits jemand genau diese Datei hochgeladen hat, dann sehen Sie die Meldung „Datei wurde bereits analysiert". Sie haben nun die Wahl zwischen „Neu analysieren" und „Zeige letzte Analyse". Meist ist es am sinnvollsten, die Datei mit den aktuellen Virensignaturen noch einmal checken zu lassen.



Viren-Check: Diese von Virustotal getestete Datei stufen 44 von 46 Virenscannern als Trojaner ein (Bild A)

Ergebnis interpretieren

Das Ergebnisfenster besteht aus mehreren Elementen: Oben steht zunächst ein Hash-Wert, der die Datei eindeutig identifiziert. Darunter stehen der „Dateiname", die „Erkennungsrate" und das „Analyse-Datum" (Bild A). Bei der Erkennungsrate zeigt die erste Zahl vor dem Schrägstrich, wie viele Scanner die



Phrozensoft Virustotal Uploader 2.2: Ziehen Sie eine Datei mit der Maus in das Fenster, um sie bei Virustotal hochzuladen (Bild B)

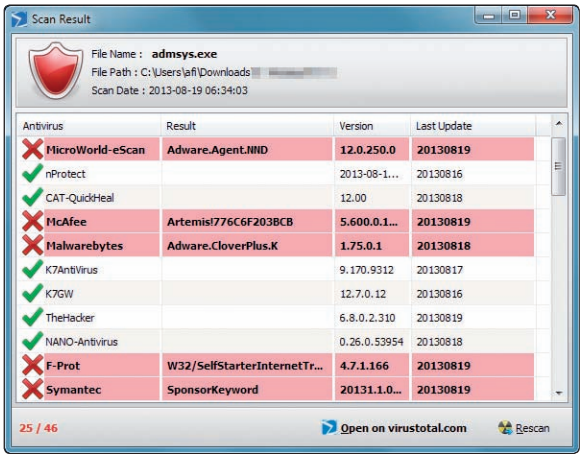
Inhalt

Tipps zu Virustotal

- **Virustotal nutzen**
  - Datei hochladen S. 134
  - Ergebnis interpretieren S. 134
- **10 Tipps zu Virustotal**
  - 1. Phrozensoft Virustotal Uploader 2.2 S. 135
  - 2. Prozesse und Dienste checken S. 135
  - 3. Dateien ohne Download checken S. 136
  - 4. Upload per Rechtsklick S. 136
  - 5. Mit Hashes suchen S. 136
  - 6. URLs scannen S. 137
  - 7. VTzilla 1.5 S. 137
  - 8. IP-Adressen checken S. 137
  - 9. Dateien per E-Mail prüfen S. 137
  - 10. Virustotal als Android-App S. 137

Datei als gefährlich einstufen. Die Zahl hinter dem Schrägstrich ist die Gesamtzahl aller Antivirenprogramme, die Virustotal eingebunden hat. Je höher die Zahl vor dem Schrägstrich ist, desto wahrscheinlicher handelt es sich um einen Schädling.

Unter „Analyse“ stehen die Ergebnisse der einzelnen Tests. Findet ein Scanner keinen Schädling, sehen Sie in der Liste ein grünes Häkchen. Erkennt der Scanner dagegen einen Virus, dann finden Sie in der Spalte „Ergebnis“ den Namen des Schädlings.



Virus gefunden: Ein Check mit Phrozensoft Virustotal Uploader 2.2 zeigt, dass diese Datei verseucht ist (Bild C)

Weil sich die Hersteller nicht auf eine gemeinsame Nomenklatur einigen können, stehen dort oft unterschiedliche Bezeichnungen. Begriffe wie „Generic“ oder „Suspicious“ besagen, dass der jeweilige Virenscanner zwar keinen Treffer in seiner Signaturdatenbank gefunden hat, die Datei aber für verdächtig hält.

Unter „File detail“ erfahren Sie etwa, ob sich jemand als „Publisher“ der Datei eingetragen hat. Außerdem steht hier, ob und welcher Packer benutzt wurde. Die Entwickler von Viren verwenden spezielle Packer für ausführbare Dateien wie UPX, um ihre Viren vor Virenscannern zu verbergen.

Unter „Zusätzliche Informationen“ stehen Infos wie verschiedene Hash-Werte, die Dateigröße und wann die Datei zum ersten Mal bei Virustotal hochgeladen wurde. Zu manchen Dateien finden sich außerdem Kommentare oder Bewertungen anderer Virustotal-Nutzer.

Die von Virustotal eingebundenen Scanner vergleichen die hochgeladenen Dateien mit Signaturen. Seit einiger Zeit blendet Virustotal bei manchen Dateien auch einen Reiter „Verhaltens-Informationen“ ein. Das heißt, diese Datei wurde in einer Sandbox ausgeführt und dort getestet. Eine Sandbox ist eine abgesicherte Umgebung, in der das Verhalten einer Datei beobachtet und aufgezeichnet wird.

10 Tipps zu Virustotal

Virustotal kann mehr als nur einzelne Dateien scannen. Lassen Sie Windows-Prozesse von dem Dienst prüfen, suchen Sie mit Hashes nach Schädlingen und sparen Sie sich so den Upload oder scannen Sie URLs.

1. Phrozensoft Virustotal Uploader 2.2

Das Tool Phrozensoft Virustotal Uploader 2.2 erleichtert den Upload von Dateien zu Virustotal und ermöglicht das Scannen von Prozessen und Diensten (kostenlos, http://phrozenblog.com/?p=259).

Installieren und starten Sie Phrozensoft Virustotal Uploader. Ziehen Sie dann verdächtige Dateien mit der Maus in das Programmfenster. Sofort lädt das Tool die Datei hoch (Bild B).

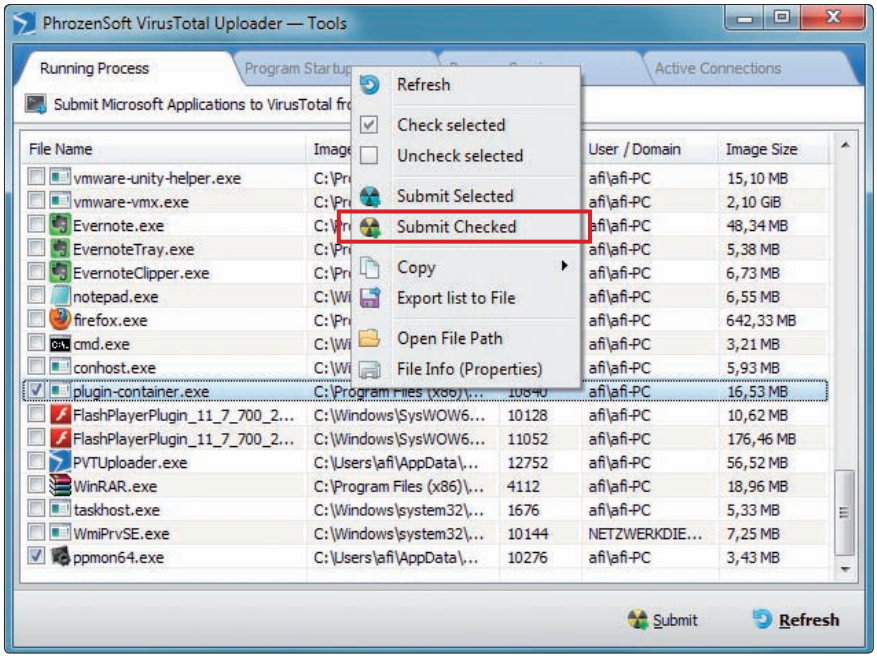
Wechseln Sie nach dem Upload zu „Available Results“ und klicken Sie doppelt auf ein Ergebnis. Ein weiteres Fenster öffnet sich, das die Rückmeldungen der Scanner zeigt (Bild C).

Wenn Sie das Ergebnis lieber auf der Virustotal-Seite sehen wollen, dann klicken Sie auf „Open on virustotal.com“.

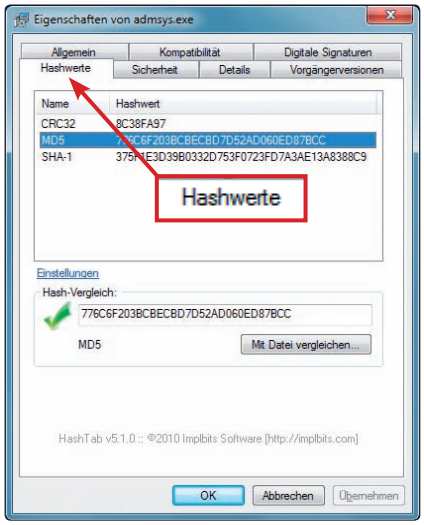
2. Prozesse und Dienste checken

Phrozensoft Virustotal Uploader 2.2 prüft auch aktive Prozesse auf Ihrem PC auf Virenbefall.

Rufen Sie dazu in dem Programm „Tools, Process Explorer“ auf. Setzen Sie anschließend Häkchen vor jedem Prozess, den Sie auf Virenbefall prüfen lassen wollen. ▶



Prozesse checken: Setzen Sie Häkchen vor verdächtigen Prozessen und laden Sie die zugehörige Datei per Rechtsklick und „Submit Checked“ bei Virustotal hoch (Bild D)



Hash Tab 5.1.0: Das Tool berechnet Hash-Werte. Nach diesen können Sie dann bei Virustotal suchen, ohne die Datei hochzuladen (Bild E)

Klicken Sie dann mit der rechten Maustaste irgendwo in das Fenster und wählen Sie „Submit Checked, Ja“ aus (Bild D). Systemprozesse von Windows sind allerdings gesperrt und lassen sich nicht hochladen.

Auf die gleiche Weise prüfen Sie mit „Program Startup“ automatisch startende Programme, mit „Program Services“ Dienste und mit „Active Connections“ aktive Netzwerkverbindungen.

3. Dateien ohne Download checken

Sie brauchen eine Datei nicht erst auf Ihren PC herunterzuladen, um sie dann wieder bei Virustotal hochzuladen und dort auf Viren prüfen zu lassen. Virustotal übernimmt auf Wunsch die ganze Prozedur für Sie.

Installieren Sie zunächst das Tool Virustotal Uploader 2.0 (kostenlos, www.virustotalcom/documentation/desktop-applications und auf). Das Programm heißt genauso wie das von Phrozensoft, wurde aber von Virustotal selbst entwickelt.

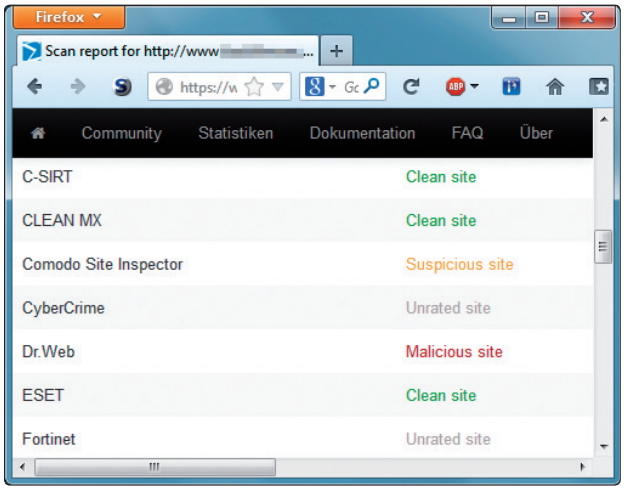
Kopieren Sie nach der Installation den Link zu der Datei in die Zwischenablage. In Firefox klicken Sie dazu mit der rechten Maustaste auf den Download-Link und wählen „Link-Adresse kopieren…“ aus. Starten Sie Virustotal Uploader 2.0 dann und klicken Sie mit der rechten Maustaste in das Feld „URL“. Wählen Sie „Einfügen“ aus. Klicken Sie dann auf „Get and Upload“.

Das Tool lädt die Datei nun, speichert sie aber nicht auf Ihrer Festplatte. Klicken Sie auf „Options“, um zum Beispiel einzustellen, dass die verdächtigen Downloads in einem speziellen Ordner gespeichert werden sollen.

4. Upload per Rechtsklick

Sie müssen nicht den Umweg über die Webseite gehen, um eine Datei bei Virustotal hochzuladen. Sowohl Phrozensoft Virustotal Uploader 2.2 als auch Virustotal Uploader 2.0 integrieren sich in das Kontextmenü des Windows-Explorers.

Die Integration von Virustotal Uploader 2.0 ist etwas besser gelungen, weil Sie beim Upload kein Fenster der Benutzerkontensteuerung von Windows bestätigen müssen: Klicken Sie mit der rechten Maustaste auf eine Datei und wählen Sie „Senden an, VirusTotal“ aus. Es öffnet sich ein kleines Upload-Fenster, das zeigt, wie die Datei hochgeladen wird. Ist der Upload fertig, öffnet sich automatisch ein Browserfenster mit dem Ergebnis.

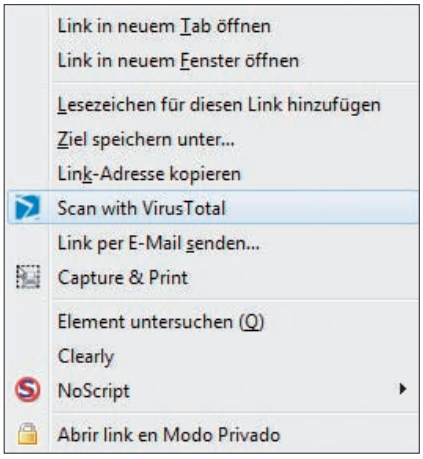


URLs scannen: Meiden Sie Webseiten, die Virustotal als „Suspicious site“ oder „Malicious site“ einstuft (Bild F)

5. Mit Hashes suchen

Ein Datei-Hash ist eine Zeichenfolge, mit der sich jede Datei eindeutig identifizieren lässt. So lautet beispielsweise der MD5-Hash für die verseuchte Datei „admsys.exe“ wie folgt: „776c6f203bcbecbd7d52ad060ed87bcc“.

Statt eine Datei bei Virustotal hochzuladen, können Sie dort auch den Hash-Wert eingeben. Gerade bei großen Dateien ist das ein nützliches Verfahren.



VTzilla 1.5: Klicken Sie mit der rechten Maustaste auf einen Link und lassen Sie die verlinkte Seite von Virustotal prüfen (Bild G)

Rufen Sie die Webseite von Virustotal auf und klicken Sie unter der Schaltfläche „Scannen!“ auf den Link „suchen“. Geben Sie den Hash-Wert in das Feld „Bedingung“ ein und klicken Sie dann auf den „Suchen!“-Button. Der Online-Dienst prüft daraufhin, ob er die Datei schon einmal getestet hat, und zeigt Ihnen anschließend das Ergebnis an.

Hash-Werte berechnen Sie mit dem Tool Hash Tab 5.1.0 (kostenlos, www.implbits.com/HashTab/HashTabWindows.aspx).

Klicken Sie nach der Installation des Tools mit der rechten Maustaste auf eine Datei und wählen Sie „Eigenschaften“ aus. Wechseln Sie zu „Hashwerte“. Markieren Sie die Zei-

le „MD5“ und drücken Sie [Strg V], um den Hash-Wert in die Zwischenablage zu kopieren (Bild E).

6. URLs scannen

Virustotal prüft nicht nur Dateien, sondern auch Webseiten auf gefährliche Inhalte. Um eine URL zu scannen, rufen Sie die Virustotal-Webseite auf und klicken auf „eine URL scannen“. Geben Sie den Link ein und klicken Sie dann auf „Scannen!“.

Auch bei diesem Dienst hat Virustotal zahlreiche Online-Scanner integriert. Sie sollten eine Seite meiden, die die Scanner als „Suspicious site“ oder „Malicious site“ einstufen (Bild F). Klicken Sie auf „Zusätzliche Informationen“, um die Gründe für die einzelnen Warnungen zu erfahren.

7. VTzilla 1.5

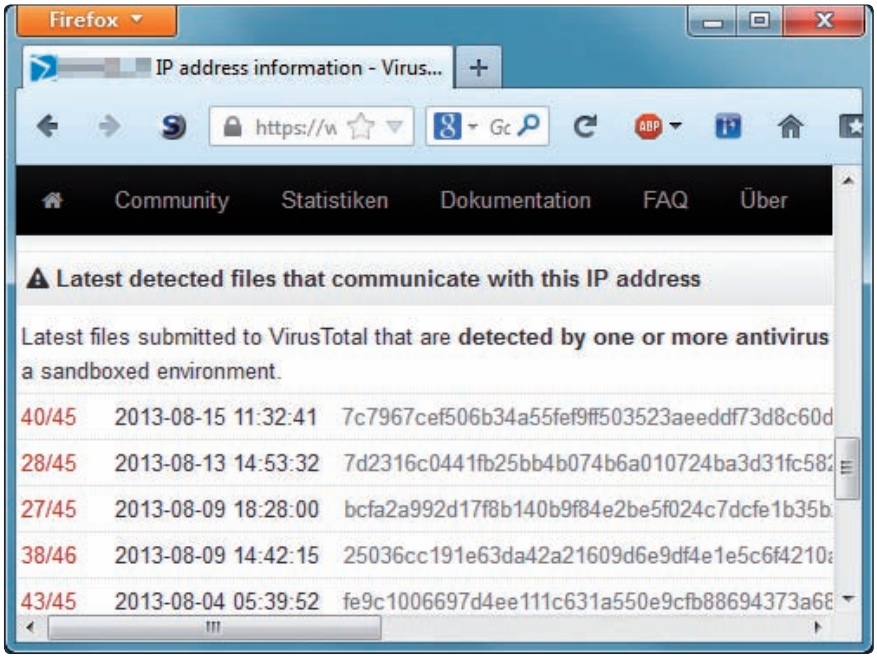
VTzilla 1.5 ist eine Virustotal-Erweiterung für Firefox, die verlinkte Webseiten prüft (kostenlos, https://addons.mozilla.org/de/firefox/addon/vtzilla und auf). Klicken Sie nach der Installation mit der rechten Maustaste auf einen Link im Browser und wählen Sie „Scan with VirusTotal“ aus (Bild G). Das Add-on öffnet einen neuen Tab, der das Ergebnis des Scans zeigt.

VTzilla erweitert den Download-Dialog von Firefox außerdem noch um die Option, eine Datei mit Virustotal zu testen.

8. IP-Adressen checken

Zu jeder IP-Adresse, die Virustotal bekannt ist, sammelt das Unternehmen Daten. So lässt sich zum Beispiel leicht herausfinden, ob Trojaner versucht haben, mit dieser IP-Adresse Kontakt aufzunehmen.

Rufen Sie www.virustotal.com/de/#search auf und geben Sie die IP-Adresse ein. Klicken Sie dann auf „Suchen!“. Wenn bei „Latest detected files that communicate with this IP address“ viele Ergebnisse auftauchen, handelt es sich vermutlich um eine gefährliche Seite (Bild H).



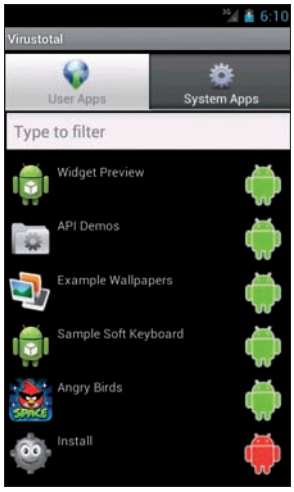
IP-Adressen checken: Mit Virustotal finden Sie auch heraus, ob eine IP-Adresse besser gemieden werden sollte. Die Liste zeigt Trojaner, die mit der IP-Adresse Kontakt aufnehmen wollten (Bild H)

9. Dateien per E-Mail prüfen

Virustotal bietet auch die Option, Dateien zu scannen, die Sie per E-Mail einsenden. Sie erhalten das Ergebnis der Virensuche dann ebenfalls per E-Mail.

Verfassen Sie eine E-Mail an den Empfänger `scan@virustotal.com`, schreiben Sie `SCAN` in den Betreff und hängen Sie die Datei an die Nachricht. Der Anhang darf nicht größer als 32 MByte sein.

Das Einsenden per E-Mail funktioniert allerdings nicht immer: Viele E-Mail-Provider haben inzwischen selbst Virenscanner auf ihren Mail-Servern installiert, die verseuchte Mails ablehnen.



Android-App: Die Virustotal-App prüft alle auf dem Smartphone installierten Apps. Rote Männchen zeigen gefährliche Apps (Bild I)

10. Virustotal als Android-App

Virustotal bietet auch eine kostenlose Android-App an, die alle Apps auf Ihrem Smartphone auf Befall mit einem Schädling testet. Suchen Sie in Google Play nach `Virustotal` und installieren Sie die App auf Ihrem Handy.

Starten Sie die App und warten Sie einen Moment, während Virustotal die Liste der installierten Anwendungen prüft. Als Ergebnis bekommen Sie zwei Listen zu sehen, einmal „User Apps“ mit den von Ihnen installierten Apps und „System Apps“ mit den vorinstallierten Apps.

Ein grünes Android-Männchen zeigt, dass die App sauber ist, während ein rotes Männchen auf eine Gefahr hinweist. Tippen Sie mit dem Finger auf einen Eintrag, um ein ausführlicheres Ergebnis zu sehen (Bild I). ■

Andreas Th. Fischer
internet@com-magazin.de

Weitere Infos

- https://groups.google.com/forum/#!forum/virustotal
  Englischsprachiges Forum zu Virustotal