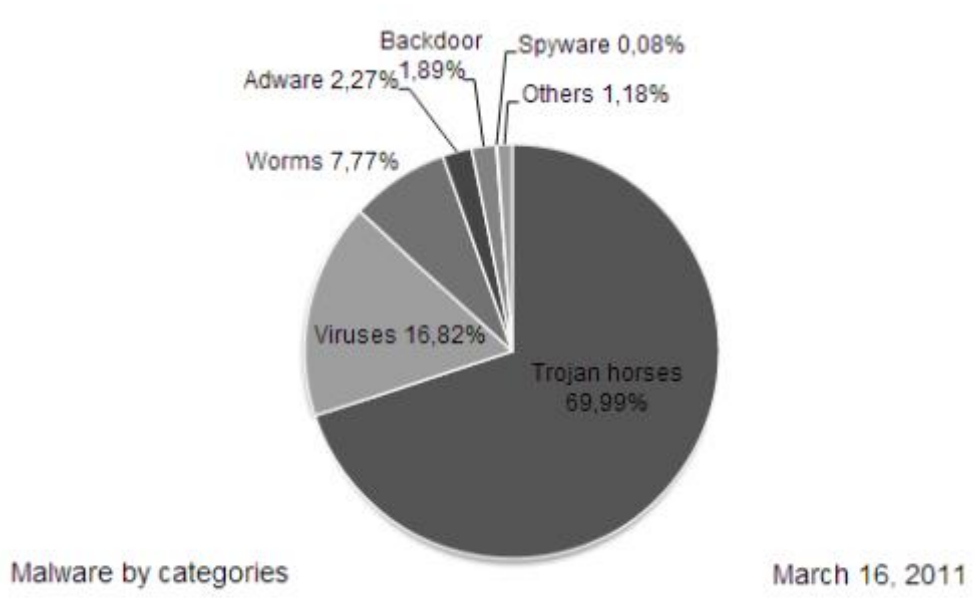
## Was ist Malware

Ob beim Fund des Anti-Viren Programms oder bei der Suche im Netz, überall taucht der Begriff Malware auf. Was das eigentlich ist, erklären wir Ihnen in diesem Praxistipp.

### Was ist Malware?



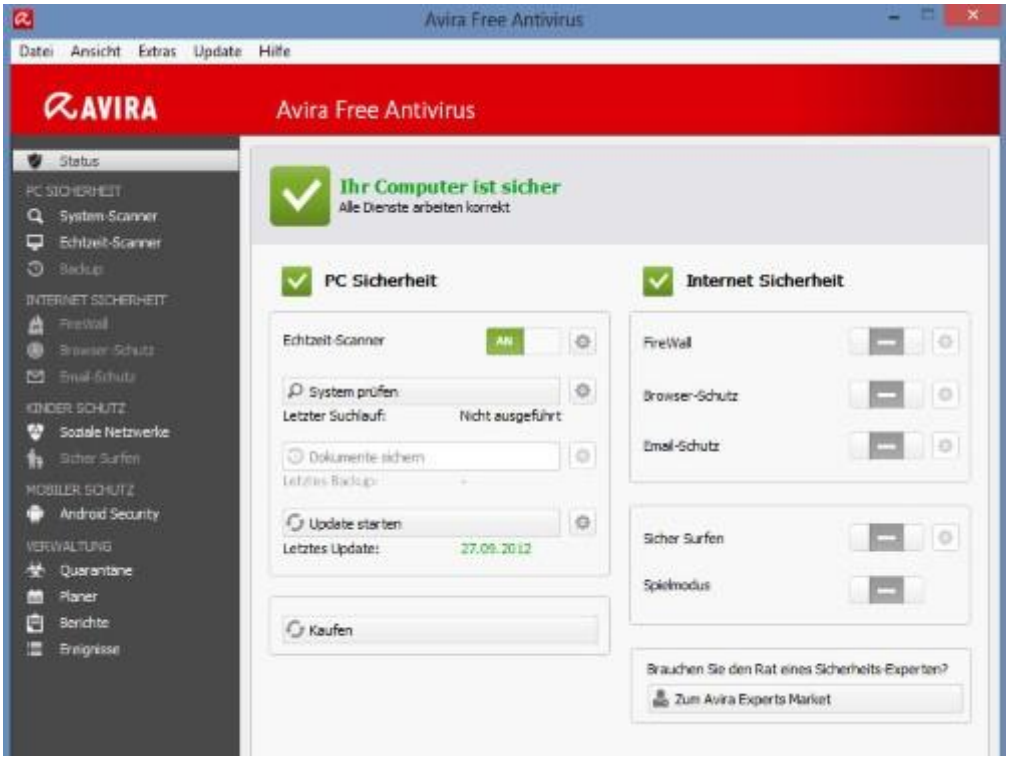

Verteilung von

Malware ist ein Sammelbegriff für Programme, die dazu entwickelt wurden Benutzern Schaden zuzufügen. Es gibt zahlreiche Unterarten von Malware – zum Beispiel, Viren, Trojaner, Rootkits oder Spyware. Alle Arbeiten anders und haben verschiedene Aufgaben. Ein Ziel haben Sie jedoch gemein: Ihnen zu schaden.

### Wie fängt man sich Malware ein?

- Malware kann praktisch überall lauern – ob im Netz beim Surfen, beim Öffnen eines Downloads oder eines E-Mail Anhangs oder beim Anschluss eines USB-Sticks. Nur selten bekommt man überhaupt mit, dass der eigene PC infiziert wurde – es sei denn Ihre Anti-Viren-Software hat die Gefahr abgewendet.
- Auch wenn überall Gefahren drohen, müssen Sie nicht gleich das Netzwerk-Kabel ziehen und das Surfen einstellen. Mit der nötigen Software und einem kritischen Blick auf Webseiten, Downloads und E-Mails brauchen Sie sich keine Sorgen zu machen.

**Wie schützt man sich vor Malware?**




Avira AntiVir

- **Anti-Viren Software**: Das A und O beim Schutz gegen Viren ist ein Anti-Viren-Programm, das auch stets Updates erhält. So sind Sie auch gegen die neusten Viren geschützt. Gute und kostenlose Software gibt es von Avira, Avast, AVG, Comodo, MSE und Bit Defender.
- **Firewall:** Die Firewall ist unter Windows bereits standardmäßig aktiviert. Sie kontrolliert alle eingehenden und ausgehenden Verbindungen und sperrt diese bei Auffälligkeiten.
- **Updates:** Damit Ihr System und auch Ihre Programme sicher bleiben, sollten Sie stets die neuesten Updates für Windows installierten und nur die aktuellen Versionen Ihrer Programme nutzen.

**Welche Arten von Malware gibt es?**

**Virus:** Ein Virus besteht aus nur einer Datei, die einen schädlichen Code enthält. Der schleust den Virus in ein Programm ein, macht es meist unbrauchbar und versucht anschließend sich weiter zu verbreiten.

**Trojaner:** Der Trojaner, wird auch als trojanisches Pferd bezeichnet, da der Nutzer sich ein vermeintlich nützliches Programm installiert, aus dem jedoch anschließend eine Bedrohung steigt. So werden meist noch andere Arten von Malware eingeschleust.

**Adware:** Die Adware ist die harmloseste Form von Viren, da Sie Ihrem System keinen richtigen Schaden zufügt. Meist nistet sie sich im Browser als Toolbar oder Add-on ein und versucht Werbung einzublenden und Ihr Surfverhalten zu beeinflussen.

**Spyware:** Die Spyware sammelt sensible Daten, die Sie auf Ihrem Computer speichern oder auch beim Online-Banking eingeben. Anschließend werden die Informationen an den Ersteller der Spyware gesendet.

**Wurm:** Ein Wurm arbeitet ähnlich wie ein Virus, befällt in erster Linie aber keine Programme. Würmer zielen eher auf den Befall von Speichermedien wie USB-Sticks und externe Festplatten ab.

**Rootkit:** Ein Rootkit gelangt meist über andere Malware wie einen Trojaner auf den PC und erlaubt dem Ersteller Zugriff auf bestimmte Teile Ihres Systems.

**Backdoor:** Diese "Hintertüren" werden durch andere Malware eingeschleust und erlauben dem Ersteller ebenfalls permanenten Zugriff auf Ihr System.

**Exploit:** Ein Exploit nutzt gezielt Sicherheitslücken im System oder in Programmen aus und kann sogar den ganzen PC kontrollieren.

**Keylogger:** Sie dokumentieren jeden Anschlag auf Ihrer Tastatur. Geben Sie beispielsweise beim Online-Banking Ihre Kontonummer und Ihren PIN ein, schickt der Keylogger die Daten an seinen Ersteller.

**Ransomware:** Diese Art von Malware sperrt mittels einer Software Teile Ihres Systems und fordert quasi Lösegeld für die Freigabe.

**Rogueware,** auch **Scareware** genannt, ist Software, die sich zum Beispiel als Viren-Scanner ausgibt. Nach dem angeblichen Fund von zahlreichen Viren verlangt das Programm den Kauf der Vollversion zur Entfernung der fiktiven Gefahren.