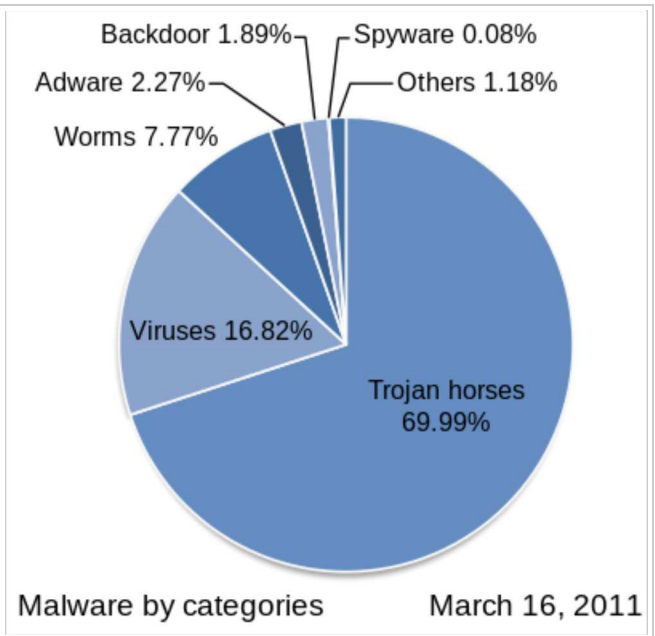
# Schadprogramm

aus Wikipedia, der freien Enzyklopädie

Als **Schadprogramm** auch **Evilware**[1], **Junkware** oder **Malware** [ˈmælˌwɛə] (Kofferwort aus englisch ***mal**icious* „bösartig“ beziehungsweise lateinisch ***mal**us* „schlecht“ und *Soft**ware***) bezeichnet man Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Malware ist damit ein Oberbegriff, der u. a. den Computervirus umfasst. Der Begriff des Virus ist älter und häufig nicht klar abgegrenzt. So ist die Rede von *Virenschutz*, womit viel allgemeiner der Schutz vor Schadsoftware jeglicher Art gemeint ist. Ein typischer Virus verbreitet sich, während die heute gängigen Schadprogramme die Struktur von Trojanischen Pferden zeigen, deren primärer Zweck nicht die Verbreitung, sondern die Fernsteuerbarkeit ist.

Mit Malware ist nicht fehlerhafte Software gemeint, obwohl auch diese selbst Schaden anrichten kann oder durch Sicherheitslücken beziehungsweise mangelnde Informationssicherheit zum Angriff auf Computersysteme ausgenutzt werden kann.




Schadprogramm-Statistik 2011. Den größten Teil nehmen Trojanische Pferde ein.

## Inhaltsverzeichnis



## Funktionsweise

Die Schadfunktionen sind gewöhnlich getarnt, oder die Software läuft gänzlich unbemerkt im Hintergrund (*Typisierung siehe unten*). Schadfunktionen können zum Beispiel die Manipulation oder das Löschen von Dateien oder die technische Kompromittierung der Sicherheitssoftware und anderer Sicherheitseinrichtungen (wie z. B. Firewalls und Antivirenprogramme) eines Computers sein, aber auch das ungefragte Sammeln von Daten zu Marketing-Zwecken. Es ist bei Malware auch üblich, dass eine ordnungsgemäße Deinstallation mit den generell gebräuchlichen Mitteln fehlschlägt, so dass zumindest Software-Fragmente im System verbleiben. Diese können möglicherweise auch nach der Deinstallation weiterhin unerwünschte Funktionen ausführen.

Für eine detaillierte Funktionsweise von Malware und insbesondere Viren → *Hauptartikel: Computervirus.*

## Klassifizierung

Bei Malware werden folgende Arten unterschieden:

- Computerviren sind die älteste Art der Malware, sie verbreiten sich, indem sie Kopien von sich selbst in Programme, Dokumente oder Datenträger schreiben. Ein teilweise defektes Virus nennt man „Intended Virus“. Dieses bewirkt meist nur eine „Erstinfektion“ einer Datei, kann sich jedoch nicht weiter reproduzieren.
- Ein Computerwurm ähnelt einem Computervirus, verbreitet sich aber direkt über Netze wie das Internet und versucht, in andere Computer einzudringen.
- Ein Trojanisches Pferd (kurz, wenn auch eigentlich falsch: „Trojaner“) ist eine Kombination eines (manchmal nur scheinbar) nützlichen Wirtsprogrammes mit einem versteckt arbeitenden, bösartigen Teil, oft Spyware oder eine Backdoor. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.
- Eine Hintertür (Backdoor) ist eine verbreitete Schadfunktion, die üblicherweise durch Viren, Würmer oder Trojanische Pferde eingebracht und installiert wird. Sie ermöglicht Dritten einen unbefugten Zugang („Hintertür“) zum Computer, jedoch versteckt

und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft genutzt, um den kompromittierten Computer als Spamverteiler oder für Denial-of-Service-Angriffe zu missbrauchen.

- *Spyware* und *Adware* forschen den Computer und das Nutzerverhalten aus und senden die Daten an den Hersteller oder andere Quellen, um diese entweder zu verkaufen oder um gezielt Werbung zu platzieren. Diese Form von Malware wird häufig zusammen mit anderer, nützlicher Software installiert, ohne den Anwender zu fragen, und bleibt auch häufig nach deren Deinstallation weiter tätig.
  - Als *Spyware* bezeichnet man Programme, die Informationen über die Tätigkeiten des Benutzers sammeln und an Dritte weiterleiten.
  - *Adware* wird Software genannt, die – häufig zusammen mit gewünschten Installationen oder Webabrufen – ohne Nachfrage und ohne Nutzen für den Anwender Funktionen startet, die der Werbung oder auch Marktforschung dienen.

- *Scareware* ist darauf angelegt, den Benutzer zu verunsichern und ihn dazu zu verleiten, schädliche Software zu installieren oder für ein unnützes Produkt zu bezahlen. Beispielsweise werden gefälschte Warnmeldungen über angeblichen Virenbefall des Computers angezeigt, den eine käuflich zu erwerbende Software zu entfernen vorgibt.

- *Ransomware* blockiert den Zugriff auf das Betriebssystem bzw. verschlüsselt potenziell wichtige Dateien und fordert den Benutzer zur Zahlung von Lösegeld auf – meist über Coupon-Bezahlsysteme wie Ukash oder Paysafecard.

- *Grayware* wird teils als eigene Kategorie benutzt, um Software wie Spyware und Adware oder andere Varianten, die Systemfunktionen nicht direkt beeinträchtigen, von eindeutig schädlichen Formen abzugrenzen (nicht zu verwechseln mit Grauware oder Reimport von Waren am offiziellen Importeur vorbei).

- Teils werden auch *Dialer* (Einwahlprogramme auf Telefon-Mehrwertrufnummern) unter Malware genannt, obwohl sie im engeren Sinne nicht dazu zählen. Illegale Dialer-Programme führen die Einwahl heimlich, d. h. im Hintergrund und vom Benutzer unbemerkt, durch und fügen dem Opfer finanziellen Schaden zu, der etwa über die Telefonrechnung abgerechnet wird. Strafrechtlich handelt es sich hier um Betrug.

- *Rogueware* (auch Rogue-Software, Rogue-Sicherheitssoftware oder englisch „rogue security software“) gaukelt dem Anwender vor, vermeintliche andere Schadprogramme zu entfernen. Manche Versionen werden kostenpflichtig angeboten, andere Versionen installieren weitere Schadprogramme während des Täuschungsvorgangs.[2][3]

# Verbreitung

Im Jahr 2008 wurden von Sicherheits-Unternehmen wie F-Secure „eine Million neuer Schädlinge“ erwartet. Täglich erreichen demnach etwa 25.000 neue Schadprogramme – sogenannte *Unique Samples*, also Schädlinge mit einzigartigem „Fingerabdruck“ nach MD5 – speziell hierfür eingerichtete Server, z. B. Honeypots. Dagegen konnte AV-Test bereits Mitte April 2008 zehn Millionen neue Schadprogramme im Jahr 2008 zählen. Es sei eine starke Veränderung bei der Verbreitung von Schadsoftware zu erkennen: Trojanische Pferde in E-Mail-Dateianhängen werden immer seltener, während die Angriffe über das Web etwa mittels Drive-by-Download zunehmen. Außerdem käme der Einsatz von Rootkit-Techniken zum Verstecken der Schädlinge immer häufiger vor.[4][5] Laut dem kalifornischen Malware-Spezialisten Kindsight Security waren 2012 in Deutschland durchschnittlich 13 % der privaten Rechner durch Malware infiziert. Nach einer Sicherheitsstudie von <kes> online und Microsoft von 2014 ist die „Infektion durch Schadsoftware“ auf den ersten Platz der Gefährdungen für die Unternehmens-IT vorgerückt. Sie hat damit „Irrtum und Nachlässigkeit der Mitarbeiter“ auf den zweiten Platz verdrängt. 74 Prozent der Studienteilnehmer hätten angegeben, dass sie in den letzten zwei Jahren von Schadsoftware-Vorfällen betroffen waren. An der Spitze der Infektionswege stehe in den befragten Unternehmen die E-Mail. Danach würden Webinhalte folgen, die die Schadsoftware über aktive Inhalte oder "Drive-by-Downloads" verteilen.[6]

### Abhängigkeit von der Verwendung freier Betriebssysteme

Während bei freier Software die Möglichkeit besteht, Sicherheitslücken durch manuelle Code-Überprüfung ("Code Auditing") zu finden und zu beheben, können Sicherheitslücken in proprietärer Software, deren Quelltext nur einem begrenzten Leserkreis zugänglich ist, nicht in jedem Fall aufgedeckt werden. Darüber hinaus beinhalten freie Betriebssysteme, beispielsweise Linux-Distributionen, häufig einen Paketmanager, in den nur Software aufgenommen wird, die gewissen Anforderungen entspricht. Zudem wird in Paketmanagern in der Regel durch Digitale Signaturen sichergestellt, dass die zu installierende Software nicht auf dem Transportweg zum Computer des Anwenders manipuliert und mit Malware versehen wird. Ein weiterer Vorteil bei der Verwendung von Paketmanagern in freien Systemen ist die Gewährleistung von Sicherheitsaktualisierungen. Sollte eine Sicherheitslücke in einem durch die Paketverwaltung installierten Programm bekannt werden, so kann diese über den Paketmanager schnell behoben werden.

# Siehe auch

- Alternativer Datenstrom
- Botnet
- Contentfilter
- Crimeware
- Dropper
- Informationssicherheit
- Keylogger