Virenscanner

Hana Salihodzic, Moritz Quotschalla, Armin Rekic

27.01.2017

Inhaltsverzeichnis

Inhalt

Definition

- Malware (engl. **mal**icious: bösartig, Soft**ware**) = Computerprogramme, die schädliche oder ungewollte Funktionen ausführen
- Schadfunktionen sind gewöhnlich getarnt, oder gänzlich unbemerkt im Hintergrund

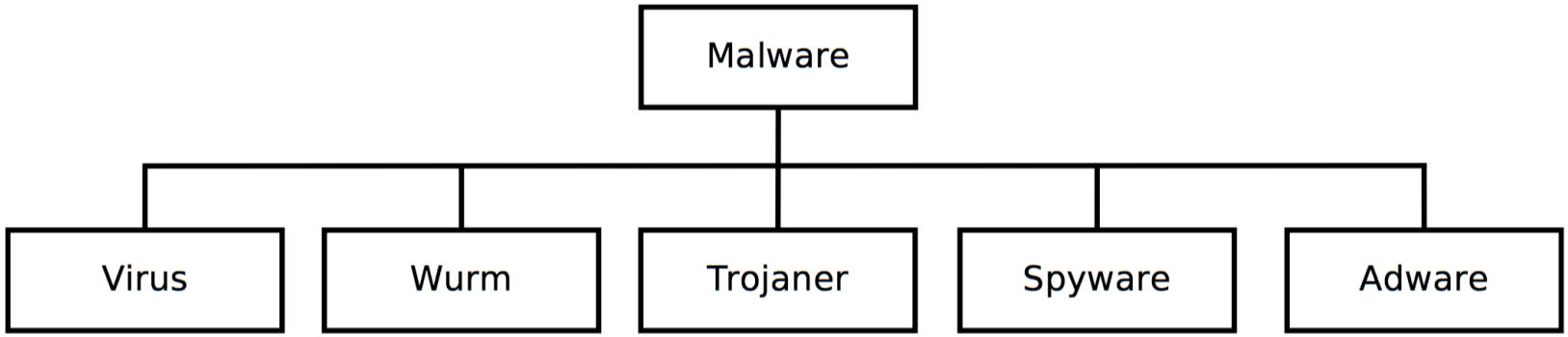

Abbildung: Wichtigste Arten von Malware

Viren

- Programme, die Kopien von sich selbst in andere Dateien schreiben
- benötigt ein Wirtsprogramm
- heutzutage sind Viren recht selten - Cyberkriminelle wollen mehr Kontrolle über die Verbreitung des Schadprogramms
- Bootviren, Dateiviren, Scriptviren usw.

Würmer

- vervielfältigt sich selbst nach der Ausführung
- anders als Viren, infizieren sie keine existierenden Dateien $\rightarrow$ sondern werden als selbständiges Programm installiert
- keine Benutzerinteraktion notwendig
- Verteilung per E-Mail, über Instant Messenger oder File-Sharing sehr üblich
- nicht-kontrollierbare Systemveränderungen als Schadfunktion

Trojaner

- gibt sich als eine sinnvolle Anwendung aus und führt unbemerkt Aktionen im Hintergrund aus
- kann nicht selbstständig verbreitet werden
- werden meist über das Internet verbreitet
- Infizierung durch Social Engineering oder Softwareinstallation
- Arten: Ransomware, Linker-Trojaner, Dropper-Trojaner, Downloader-Trojaner
- Klassiker sind gefälschte Antivirenprogramme

Spyware

- Programme, die ohne Genehmigung und Wissen des Benutzers Informationen sammeln und diese dann weiterleiten
- gezielte Werbung wird angezeigt
- Adware: Freeware, die über die Einblendung von Werbung finanziert wird, zeigt während der Benützung ständig Banner oder andere Werbeeinblendungen an

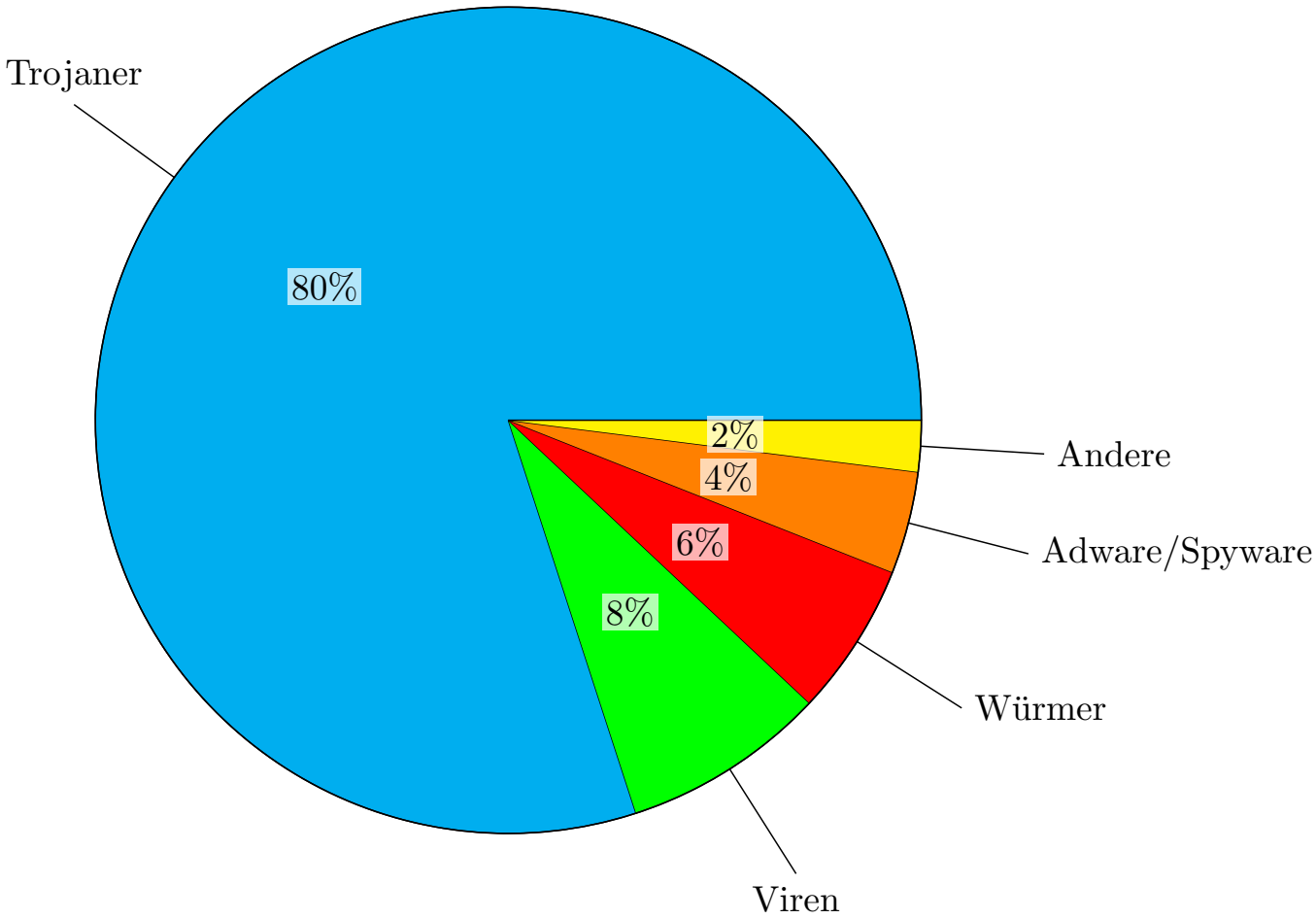

Abbildung: Malware-Infektionen im Jahr 2016

Abbildung: Aktuelle Berichte über Malware-Attacken 2016

Inhalt

Statistiken

Abbildung: Weltweit infizierte Computer

Insgesamt entstand im Jahr 2015 durch Cyberkriminalität weltweit ein volkswirtschaftlicher Schaden von 500 Milliarden Euro.
- Munich Re

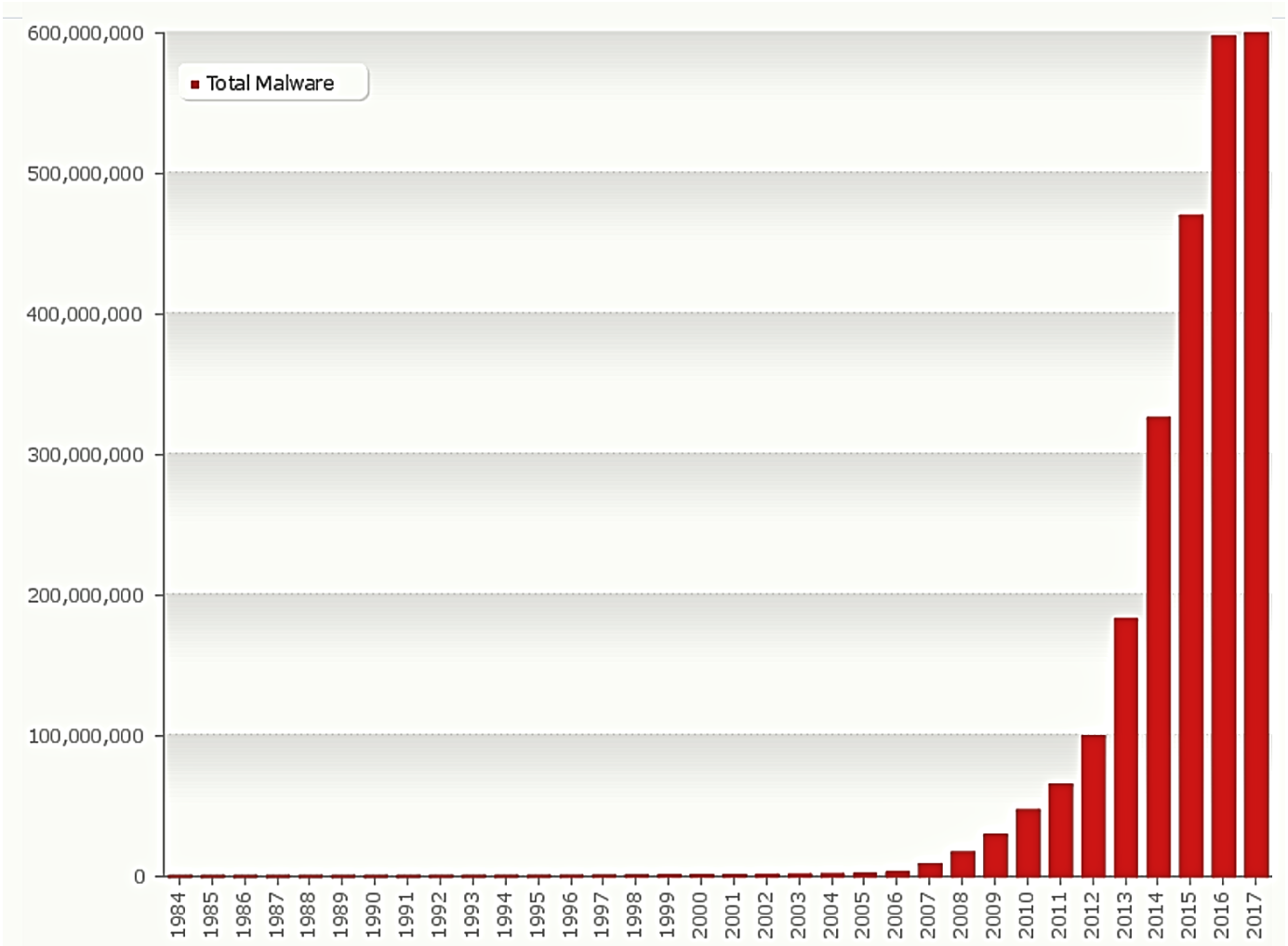

Abbildung: Vorkommen von Malware in den letzten 30 Jahren

Inhalt

Manueller Scanner (On-Demand-Scanner)

- muss vom Benutzer manuell gestartet werden
- gefundene schädliche Software wird auf Wunsch in Quarantäne verschoben oder gelöscht
- sollte regelmäßig durchgeführt werden

Echtzeitscanner (On-Access-Scanner)

- im Hintergrund als Systemdienst aktiv
- scannt alle Dateien, Programme, den Arbeitsspeicher und evtl. HTTP/FTP-Verkehr
- Filtertreiber werden installiert $\rightarrow$ Schnittstelle zwischen Echtzeitscanner und Dateisystem
- zwei Strategien
  - Scannen beim Öffnen von Dateien (Lesevorgang)
  - Scannen beim Erstellen/Ändern von Dateien (Schreibvorgang)

Online-Virenscanner

- Programmcode und Viren-Signaturen werden online geladen
- Großteil der Datenanalyse ist ausgelagert
- arbeiten nur im On-Demand-Modus
- oft als Second-Opinion-Scanner benutzt
- abhängig vom Internet

Inhalt

Wie kann die Erkennung erfolgen?

- Reaktive Methoden:
  - nutzen Kenntnisse über bestehende Malware, um sie zu erkennen und neue Infektionen zu vermeiden
  - zuverlässiger Schutz gegen bekannte Bedrohungen
- Proaktive Methoden:
  - versuchen Malware anhand von verdächtigem Verhalten zu identifizieren
  - deutlich leistungsintensiver
  - höhere Fehlerquote

Signaturbasierte Erkennung

- integrierte Bibliothek mit sog. Virensignaturen
- werden verwendet, um bereits bekannte Malware eindeutig zu identifizieren
- zuverlässige Erkennung, selten Fehlalarme (false-positive)
- bei geringer Veränderung lässt sich der Virus oft nicht mehr erkennen
- Aktualität ist wichtig $\rightarrow$ täglich/wöchentlich Updates
- gründliche Analyse neuer Malware nötig

Heuristische Erkennung I

- untersucht Programme auf Struktur und Verhalten hin
- Malware enthält oft Schadfunktionen (z.B. Löschen von Dateien) oder Verbreitungsmethoden (Versenden von infizierten E-Mails)
- werden mehrere solcher Merkmale gefunden, wird die Ausführung gestoppt
- ermöglicht Erkennung von bisher unbekannter Malware auch ohne Update

Heuristische Erkennung II

- fehleranfälliger als signaturbasierte Erkennung
- Updates aufwendiger und seltener als bei Virensignaturen

Sandbox I

- Testen der Dateien, die bisher nicht negativ aufgefallen sind
- eignet sich vor allem für Downloads oder E-Mail-Anhänge
- isolierter Bereich, in dem Programme ausgeführt werden
- Analyse, welche Aktionen durchgeführt werden, ohne Schaden am wirklichen System anzurichten
- Erwartung einer für diese Datei typische Verhaltensweise $\rightarrow$ andernfalls Kennzeichnung als potentielle Gefahr

Sandbox II

- ähnelt Emulation eines separaten Betriebssystems in einer virtuellen Maschine
- unbekannte Malware kann möglicherweise ohne Signatur erkannt werden
- fortschrittliche Malware erkennt, ob sie in einer Sandbox ausgeführt wird und verhält sich dann unauffällig

Verhaltensanalyse I

- im Gegensatz zu Sandboxing und Heuristik erst nach dem Programmstart und nicht in einem abgetrennten Bereich
- beobachtet fortlaufend Verhalten von ausgeführten Prozessen
- schreitet ein, wenn bestimmte Verhaltensregeln durch Prozesse verletzt werden
- kann Infektion nur eindämmen, aber nicht verhindern

Verhaltensanalyse II

- gute Verhaltensanalysen achten auf den Kontext und nicht auf einzelne Aktionen
- Optimierung in Kombination mit künstlicher Intelligenz (z.B. neuronale Netze) $\rightarrow$ bessere Erkennungsrate

Inhalt

Unterschiede bei Betriebssystemen I

- Windows:
  - am meisten verbreitetes Betriebssystem, daher sehr attraktiv
  - Windows Defender schneidet schlecht in Tests ab
  - Virenscanner sind bei Windows ein Muss
- Mac:
  - allgemein sicherer als Windows
  - Mac eigener Schutz: Gatekeeper, Sandbox und Xprotect zuverlässig
  - Zahlenmäßig viel weniger Angriffe auf Mac als auf Windows

Unterschiede bei Betriebssystemen II

- Linux:
  - für Hacker recht uninteressant
  - wenige Nutzer und viele, verschiedene Distributionen
  - bietet kaum Angriffsflächen, da Skripte aus dem Netz nicht automatisch starten können
  - Systembeschränkungen - keine 'Admin'-Rechte
  - Lücken werden schneller und regelmäßig gestopft
  - Kein Virenscanner notwendig

Mobilgeräte I

- Android:
  - keine strenge Kontrolle der Apps im PlayStore
  - andere Drittanbieter Quellen sind erlaubt
  - Virenscanner ist zu empfehlen
- iOS:
  - geschlossene Umgebung
  - genauere Kontrolle der Apps im App Store
  - kein Virenscanner nötig
  - Ausnahme: iOS mit 'Jailbreak'

Inhalt

Virenscanner im Vergleich I

- Schutzwirkung:
  - Schutz gegen Zero-Day Malware angriffen aus dem Internet inkl. bösartiger Websites/E-Mails
  - Erkennung von weit verbreiteter und häufig vorkommender Malware aus den letzten 4 Wochen
- Geschwindigkeit:
  - Aufruf von populären Seiten
  - Downloads/Installation von häufig genutzten Programmen
  - Kopieren von Dateien (Lokal und im Netz)

Virenscanner im Vergleich II

- Benutzbarkeit:
  - Ablenkung des Benutzers durch Warnmeldungen bei unbekannten Programmen oder aufgrund eines Fehlalarms
  - Fälschliche Erkennung von gutartigen Programmen als schädliche Software
- Reparaturleistung:
  - Fähigkeit beim Entfernen von Schadsoftware
  - Sanierung von weiteren Systemveränderungen
  - Aufspüren und Entfernungsleistung bei speziell versteckter Software (Rootkits)

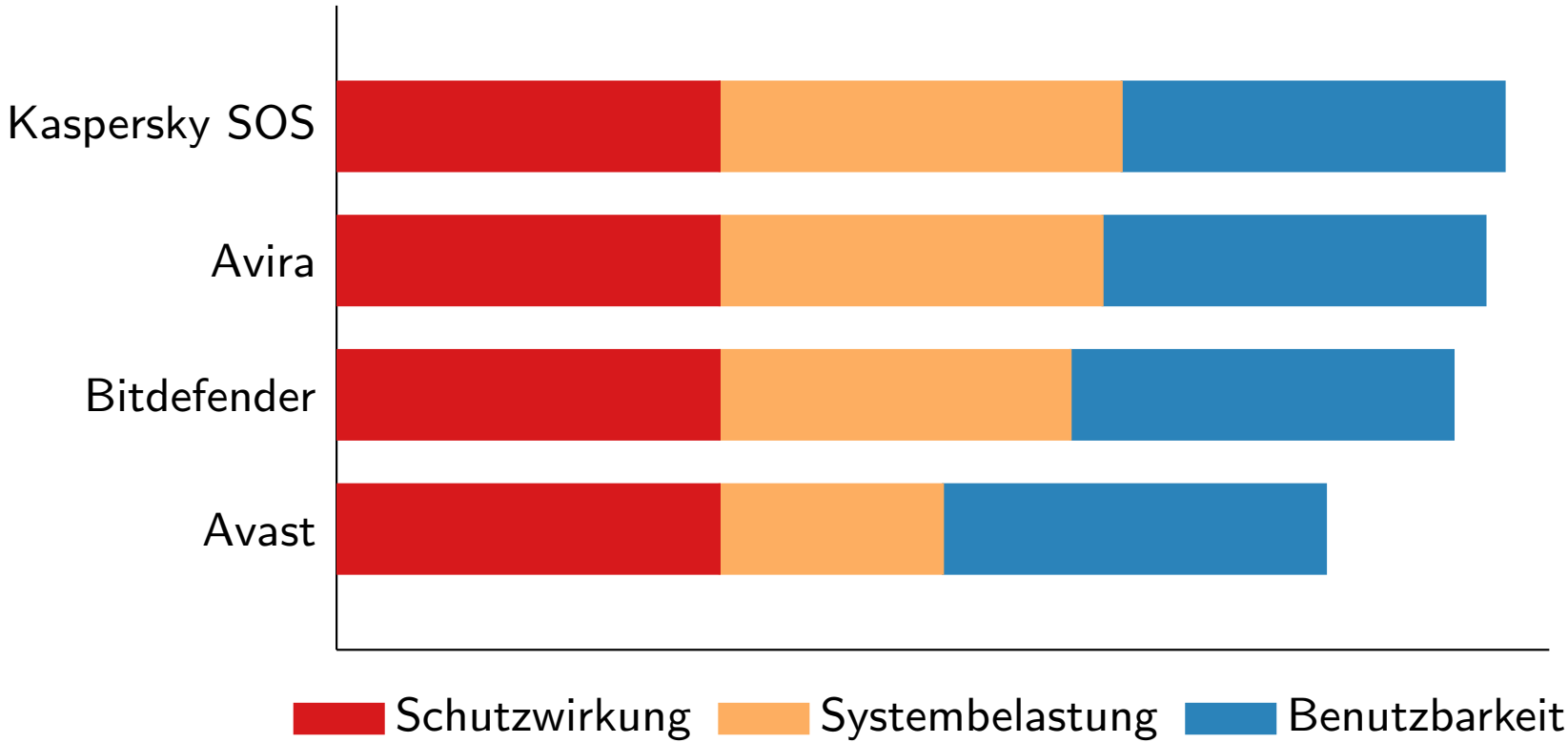

Abbildung: Virenscanner Ranking (gemäß https://www.av-test.org)

- Ranking:
  - 1. Kaspersky Internet Security 39.95€/Jahr
  - 2. Avira Antivirus Pro 34.95€/Jahr
  - 3. Bitdefender Internet Security 59.99€/Jahr (3 Geräte)
- Bester kostenloser Scanner:
  - Avast Free Antivirus
  - jedoch muss man Qualitätseinbußen hinnehmen

Schutzfunktion	Kostenloses Programm	Kostenpflichtiges Programm
Schutz vor bekannten Schädlingen	✔	✔
Guter Schutz vor unbekannten Schädlingen	✖	✔
Notfall-Bootmedium	✖	✔
Schutz in sozialen Netzwerken	✖	✔
Sicherheit bei Online-Transaktionen	✖	✔
Firewall Internetschutz	✖	✔
E-Mail Werbefilter	✖	✔
Kinderschutz	✖	✔
WLAN-Schutz	✖	✔

Abbildung: Kostenlos vs. Kostenpflichtig

Nachteile

- Dateien müssen immer erst gescannt werden:
  - führt zu Verzögerungen bei manchen Anwendungen
  - eventuell sogar zu Funktionsstörungen
- Ungefährliche Datei wird fälschlicherweise als Malware identifiziert $\rightarrow$ false positives
- Virenscanner, welche infizierte Dateien sofort löschen, können zu Problemen führen
  - Mai 2007: Symantec, aufgrund fehlerhafter Virensignatur irrtümlicherweise grundlegende Betriebssytemdateien gelöscht $\rightarrow$ tausende PCs konnten nicht mehr booten
  - Oktober 2011: Microsoft Security Essentials entfernten Google Chrome, der als 'Zbot banking trojan' klassifiziert wurde

Vielen Dank für die Aufmerksamkeit!

Quellen

- www.wikipedia.org
- www.blog.kaspersky.de
- www.edv-lehrgang.de/malware
- www.spam-info.de/viren
- www.computerlexikon.com/was-ist-virenscanner
- www.av-test.org/de/statistiken/malware
- www.pandasecurity.com
- www.netzsieger.de
- arxiv.org/ftp/arxiv/papers/1104/1104.1070.pdf
- www.antivirenprogramm.net
- www.cschmidt-computerservice.de/it-security
- public.gdatasoftware.com