anti Virus Test Center (aVTC)
Fachbereich Informatik
Universität Hamburg

Klassifikation von bösartiger Software und aktuelle Testergebnisse des Virus Test Centers von AntiMalware-Software unter Linux

Bodo Eggert, Michel Messerschmidt, Jan Seedorf
Linuxtag 2003

Inhalt

- Teil A: Definitionen und Klassifikation von bösartiger Software
  (Jan Seedorf)
- Teil B: Einfallstore für Malware und Beispiele unter Linux
  (Bodo Eggert)
- Teil C: Testergebnisse des aVTC von Antimalware-Produkten unter Linux
  (Michel Messerschmidt)

Das antiVirusTestCenter der Universität Hamburg

- Fachbereich Informatik, Universität Hamburg
- Leitung: Prof. Dr. Klaus Brunnstein
- Regelmäßige Tests von AntiMalware-Software seit 1992
- Zur Zeit Tests unter Linux, Windows98, Windows2000 und WindowsXP
- Testbedingungen, -methodik und -ergebnisse werden veröffentlicht: **www.avtc.info**
- Studenten lernen Umgang mit bösartiger Software und das wissenschaftliche Testen von Anti-Malware-Software

Definitionen und Klassifikation von bösartiger Software

- Bedrohungen in vernetzten Computer-systemen
- Definition Malware / bösartige Software
- Klassifikation von Malware
- Definition Virus
- Klassifikationen von Viren

Bedrohungen in vernetzten Computersystemen

- Verlust von Daten
- Unbefugter Zugriff auf lokale Daten (aus dem Netzwerk)
- Unbefugter (eventuell unbemerkter) Versand von sensitiven Daten
- Unbefugte (eventuell unbemerkte) Veränderung von lokalen Daten (aus dem Netzwerk)
- Datenspionage bei Versand von Daten über ein Netzwerk
- Adressfälschung
- Verhinderung des Zugriffs auf Dienste im Netzwerk (denial of service)

Definition Malware / bösartige Software

Definition:

"A software or module is called "malicious" ("malware") if it is intentionally dysfunctional, and there is sufficient evidence (e.g. by observation of behaviour at execution time) that dysfunctions may adversely influence the usage or the behaviour of the original software."

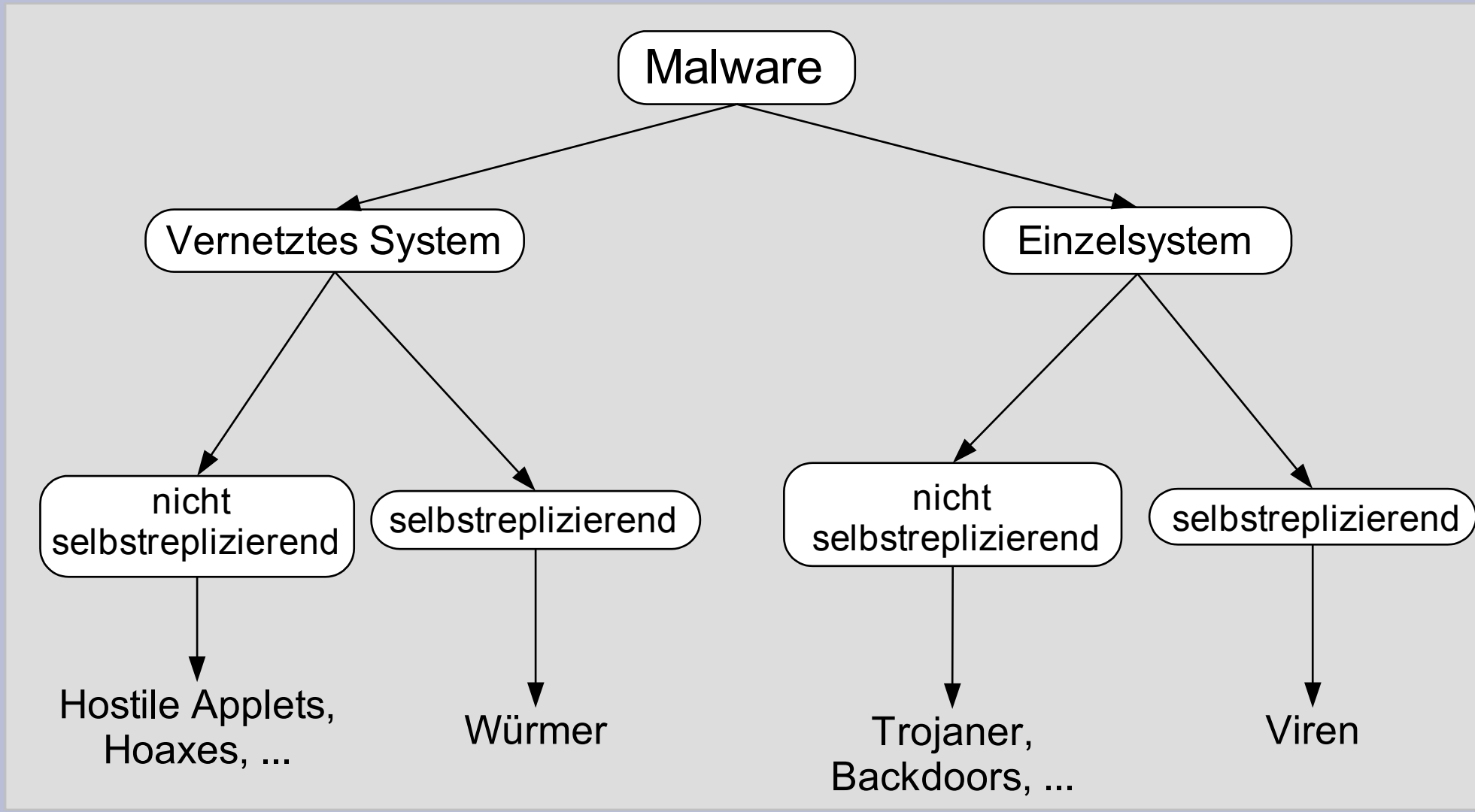
([Brunnstein 1999])

Definition Malware / bösartige Software

Malware:

- fasst als Oberbegriff alle Arten von bösartiger Software zusammen, die für Benutzer eine Gefahr darstellt
- Bezeichnung für *intentional dysfunktionale* Software
- Dysfunktional: Software, die von der (formalen oder informalen) Spezifikation abweicht und somit für den Anwender "unerwünschte und unerwartete Funktionen besitzt"
- Intentional: die zusätzlichen, verborgenen Funktionalitäten sind vom Programmierer der Software beabsichtigt
- beinhaltet als Begriff nicht so genannte "Bugs"

Klassifikation von Malware



Definition Virus

Definition:

"Any software that reproduces (or "self-replicates"), possibly depending on specific conditions, at least in 2 consecutive steps upon at least one module each (called "host") on a single system on a given plattform, is called a "virus" (for that plattform). A virus may be compiled (e.g. boot and file virus) or interpreted (e.g. script virus)."

([Brunnstein 1999])

Definition Virus

Virus:

- Malware, die durch Infektion andere Dateien befällt und sich so reproduziert
- befallene Datei heißt *Wirtsdatei*
- Ein ***Virus*** verbreitet sich auf ***lokalen*** Systemen
- verbreitet sich maliziöse Software selbstständig über ***Netzwerke***, so wird sie als ***Wurm*** bezeichnet

Klassifikationen von Viren

- Klassifikation nach Plattform
  - Boot-Viren (engl. boot viruses)
  - Datei-Viren (engl. file viruses)
  - Makro-Viren (engl. macro viruses, z. B. .doc, .xls)
  - Skript-Viren (engl. script viruses, z. B. .js, .vbs)
- Klassifikation nach Verbreitung
  - Monatliche Liste von der WildList Organisation (www.wildlist.org)
  - Unterscheidung von Viren danach, ob sie „in-the-wild“ sind oder nicht

Einfallstore für Malware

Beispiele für Verbreitung:

- Lokale Verbreitung, Social Engineering
- Freigaben
- Wechseldatenträger
- Buffer Overflow (zu lange Eingabedaten)
- Auswertung im falschen Kontext
- Unzureichende Prüfung der Zugriffsrechte, Ausnutzung einer Vertrauensstellung

➔ In wie weit schützen Virusscanner ?

Einfallstore für Malware

- Lokale Verbreitung, Social Engineering
  - Infizerte Programme
  - „Klick mich, ich bin ein Bild von Anna Kournikova!.jpg.vbs“

    ```
    Gut erkennbar, Malware liegt als Programmdatei vor.
    ```

  - Hoaxe

    ```
    Harmloser Text wird vom Benutzer ausgeführt und mit
    neuer Formatierung weitergeleitet
    -> Kein Ziel für Virusscanner!
    ```

Einfallstore für Malware

- Freigaben mit Schreibrechten
  - Systemverzeichnisse

    Die Schadsoftware kann sich in den Startmechanismus einfügen und den Virusscanner sabotieren.
    Zum Entdecken muß man die Datei beim Schließen scannen.
  - Downloadverzeichnisse

    Virus kann sich als „setup.exe“ ablegen oder diese ersetzen.

    On-Demand-Scanner schützen nicht zuverlässig.

Einfallstore für Malware

- Wechseldatenträger
  - Boot-Viren

    Virusscanner läuft noch nicht beim Systemstart
    Moderne Betriebssysteme umgehen BIOS und Viren

    -> Verbreitung mögich, bis Betriebssystem geladen ist
  - Autostart-Funktion

    Schadsoftware ist erkennbar wie normale infizierte Dateien, aber On-Access-Scanner sind hier ungeeignet.

Einfallstore für Malware

- Buffer Overflow (zu lange Eingabedaten)

  Der maliziöse Code läuft zunächst im Hauptspeicher ab, ein Virusscanner wird diesen jedoch normalerweise nur beim Systemstart scannen.

  Ist der Auslöser des Buffer-Overflows eine Datei, so kann diese erkannt werden. Auch nachgeladene Dateien können erkannt werden.

  Netzwerkverkehr wird noch nicht überwacht
  -> manche Würmer können nicht erkannt werden.

Einfallstore für Malware

- Auswertung im falschen Kontext
  - Daten werden als Programm ausgewertet

    ```
    GET /cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
    ```

  - Daten werden vom falschen Programmteil ausgewertet

    ```
    Mime-Exploit in Outlook:

    Musik und als Musik gekennzeichnete Programme werden
    automatisch ausgeführt
    ```

Einfallstore für Malware

- Unzureichende Prüfung der Zugriffsrechte, Ausnutzung einer Vertrauensstellung
  - IFrame: Auswertung ohne Prüfung
  - Morris-Wurm: Verbreitung zu Accounts auf anderen Hosts über r-Dienste

```
Virusscanner sind wie bei Buffer-Overflows auf ein
scannbares Objekt angewiesen.
```

Beispiele für Malware unter Linux

- Slapper
  - Verbreitung über OpenSSL-Exploit in Apache/mod_ssl
  - Verwundbarkeit bekannt seit August 2002
  - Aufgetreten am 13. September 2002
  - Enthält DDoS-Funktionen
- Verbreitung

1) Opfer identifizieren: Abfrage auf Port 80
2) „Apache“? -> Exploit-String an Port 443 (SSL)
3) Programm nachladen, decodieren, compilieren und ausführen

Beispiele für Malware unter Linux

- Winux
  - alias Lindows, PEELF
  - Proof-of-Concept
  - Infiziert ELF- und PE-Dateien
  - Reparatur trivial

Testergebnisse des aVTC

- Der aVTC-Test 2002-12
- Verwendete Malware-Testbeds
- Getestete Produkte unter Linux
- Testergebnisse
  - Das beste Produkt ?
  - „Zoo“-Viren
  - „In-The-Wild“-Viren
  - nicht-selbstreplizierende Malware
  - Falschmeldungen
  - Viren in komprimierten Dateien
  - Bewertung der Linux-Ergebnisse

Der aVTC-Test 2002-12

- Tests unter Windows 98, Windows 2000, Dos und SuSE Linux 7.1
- Getestet wurden insgesamt 20 Antimalware-Produkte, davon 8 unter Linux
- Testumfang:
  - 12 verschiedene Malware-Testbeds
  - ca. 40.000 verschiedene Viren/Malware
  - mehr als 200.000 infizierte Dateien (Samples)

Verwendete Malware-Testbeds

- „In-The-Wild“-Viren:
  - File
  - Makro
  - Skript
  - Boot (nur unter DOS)
- „Zoo“-Viren
  - File
  - Makro
  - Skript
- Nicht-selbstreplizierende Malware
  - File
  - Makro
  - Skript
- „In-The-Wild“-Viren in komprimierten Dateien
  - File
  - Makro

Zusätzlich enthalten einige Datenbanken noch „false positives“

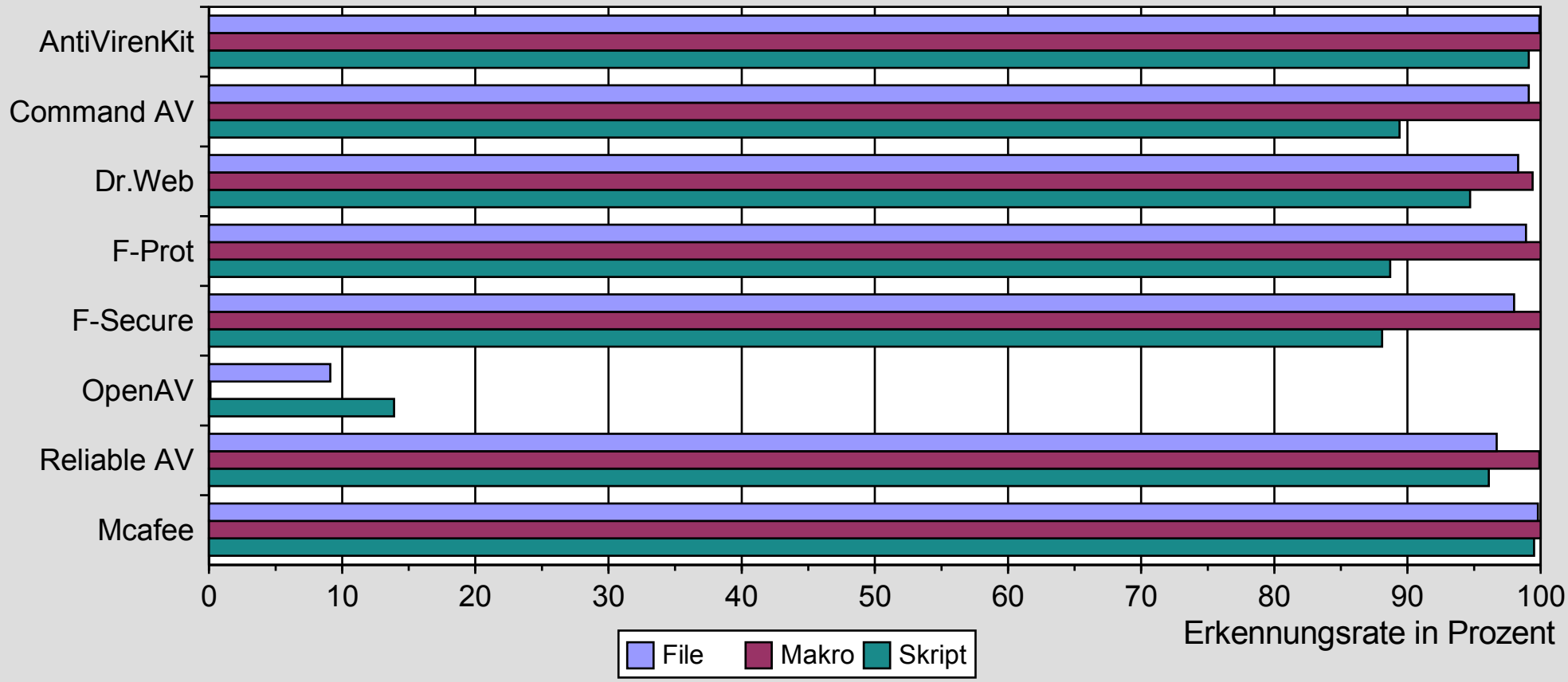
Getestete Produkte unter Linux

- GData AntiVirenKit 10
- Command Antivirus 4.64.1
- Dr.Web for Linux 4.26
- F-Prot for Linux 3.11b
- F-Secure Antivirus 4.13 build3360
- OpenAntiVirus ScannerDaemon 0.2.0
- Reliable Antivirus 8.3.1
- McAfee Viruscan 4.16.0

Testergebnisse

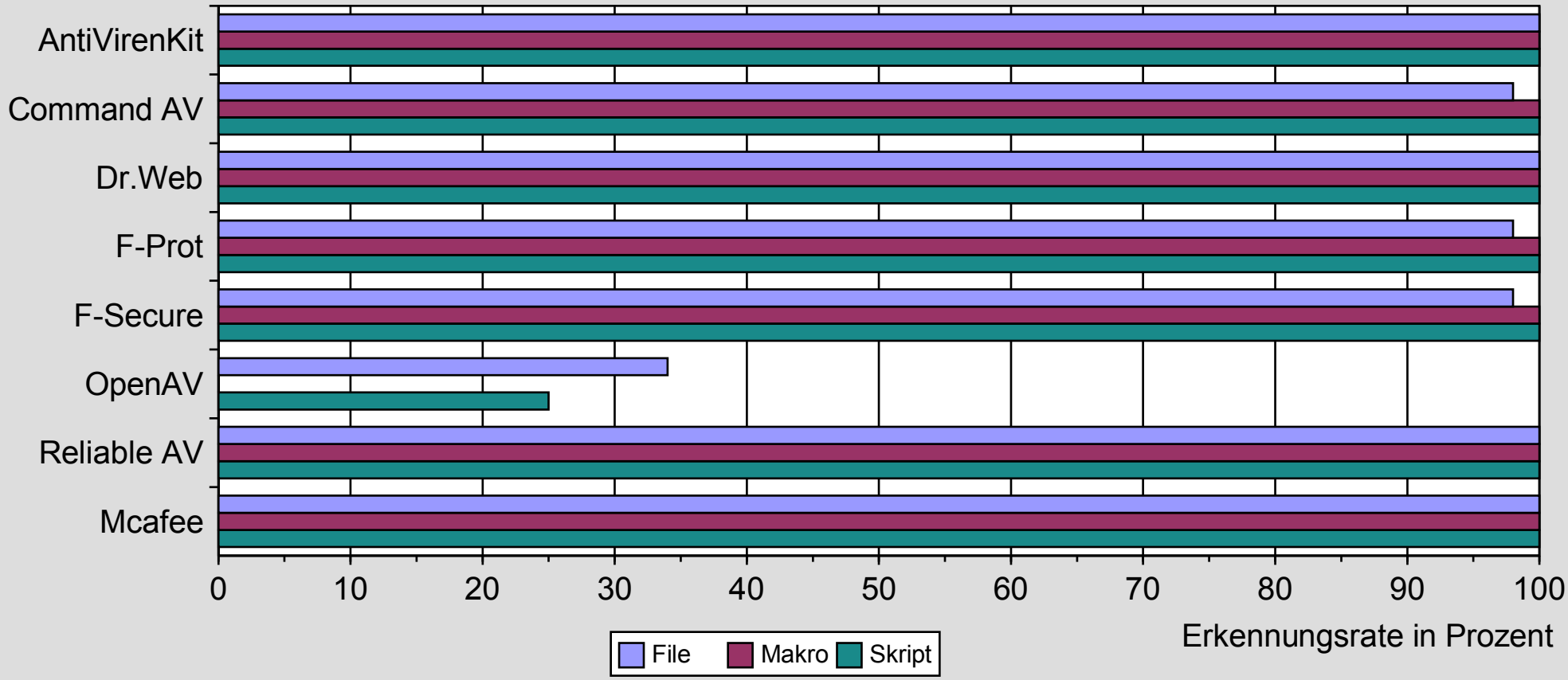
- „Was ist das beste Produkt ?“
  - meist die erste Frage bei Produkttests
  - ist abhängig vom Einsatzbereich
  - setzt umfassenden Test **aller** relevanten Aspekte eines Produkts voraus
  - wird deshalb von den aVTC-Tests nicht beantwortet
- Tests des aVTC ermitteln die Erkennungsrate
- Produkt-Bewertung erfolgt nur unter diesem Aspekt

Testergebnisse:
„Zoo“-Viren



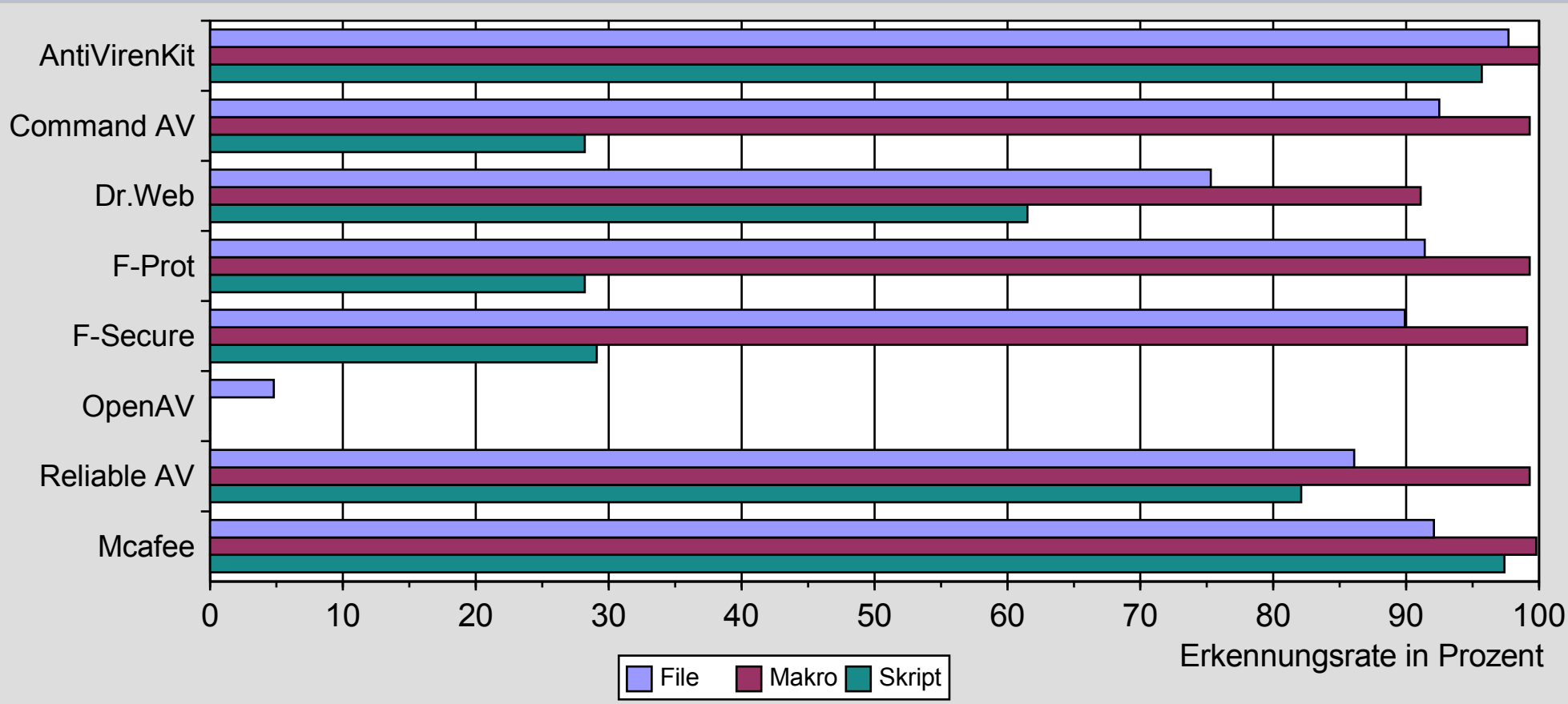
- Command, F-Prot und F-Secure zeigen deutliche Schwächen bei Skript-Viren
- Reliable AV hat leichte Schwächen bei File-Viren (immerhin über 700 Viren nicht erkannt)

Testergebnisse:
„In-The-Wild“-Viren



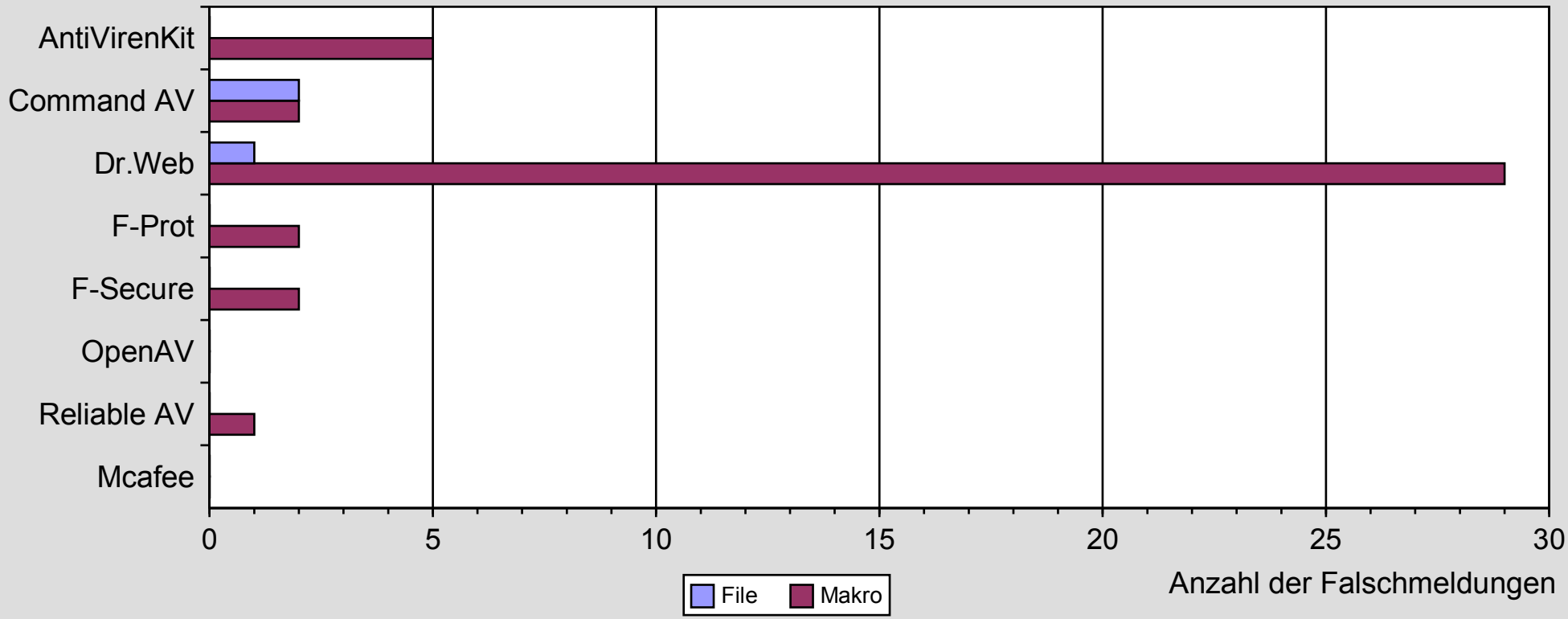
- Command, F-Prot und F-Secure erkennen genau einen File-Virus gar nicht
- Dies ist aber als mindestens genauso schwerwiegend einzustufen wie die 700 von Reliable AV nicht erkannten Viren in den Zoo-Datenbanken

Testergebnisse:
nicht-selbstreplizierende Malware



- Hier erreichen nur AntiVirenKit und Mcafee akzeptable Erkennungsraten

Testergebnisse:
Falschmeldungen



- Viele Produkte haben anscheinend Probleme, schädliche und harmlose Makros in Office-Dokumenten zu unterscheiden
- Lediglich Mcafee zeigt eine gute Leistung
- OpenAV sieht zwar ebenfalls gut aus, erkennt allerdings gar keine Makroviren

Testergebnisse:
Viren in komprimierten Dateien

In folgenden Archiv-Formaten wurden „In-The-Wild“-Viren erkannt:

	Zip	Arj	Cab	Lha	Rar 1.5	Rar 2	Rar 3
AntiVirenKit	ja	ja	ja	ja	ja	ja	nein
Command AV	ja	ja	ja	ja	ja	ja	nein
Dr.Web	ja	ja	ja	nein	ja	ja	nein
F-Prot	ja	ja	ja	ja	ja	ja	nein
F-Secure	ja	ja	nein	ja	nein	nein	nein
OpenAV	nein	nein	nein	nein	nein	nein	nein
Reliable AV	ja	ja	ja	nein	ja	ja	ja
Mcafee	ja	ja	ja	ja	ja	ja	nein

- Bei einigen Produkten ist die Erkennung in Archiven allerdings nicht sehr zuverlässig

Bewertung

- Alle gezeigten (und weitere) Kategorien werden getrennt bewertet und mit unterschiedlicher Gewichtung zu einem Gesamtergebnis summiert.
- Von maximal 24 Punkten erreicht:
  - Mcafee 21 Punkte
  - AntiVirenKit 19 Punkte
  - Dr.Web, Reliable AV 11 Punkte
  - Command, F-Prot 10 Punkte
  - F-Secure 7 Punkte
  - OpenAV 0 Punkte

Vielen Dank für die Aufmerksamkeit

Fragen ?

Ausführliche Beschreibung der Testergebnisse und Testmethodik:

www.avtc.info