

# **Businessmalware**

## **Wenn Signaturen nicht genügen**

Magnus Kalkuhl,  
Virus Analyst Kaspersky Labs GmbH

## Definition

### **Business Malware**

ist bösartige Software,  
die gezielt zur Schädigung  
von Unternehmen eingesetzt wird

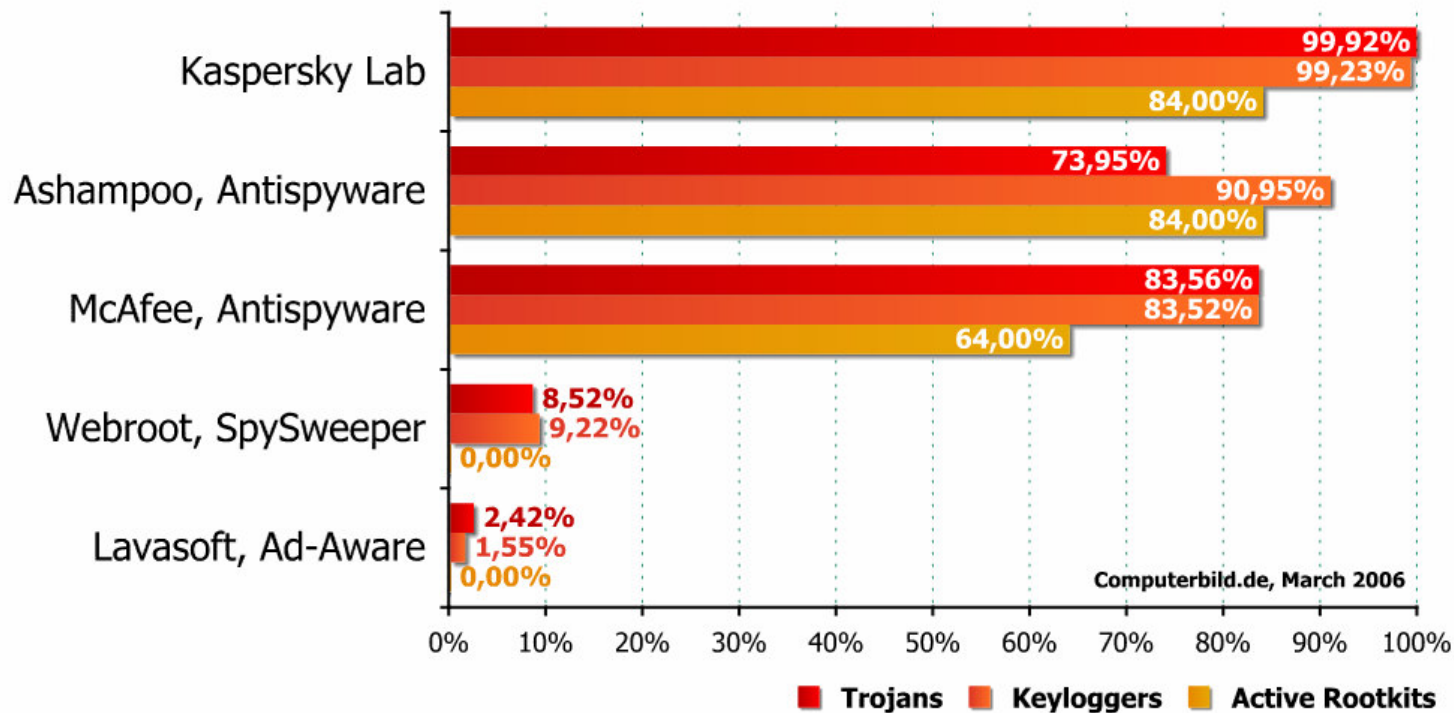
## Warum hört man so selten davon?

- ❖ Die meisten Unternehmen wissen nicht, dass sie überhaupt ein Problem haben
- ❖ Diskretion, um Imageschäden zu vermeiden
- ❖ Die Presse interessiert sich nur für die großen Fälle

## Viele Wege, ein Ziel

- ❖ Vermeintliche Werbe-CDs  
(2005: Israelische Unternehmen werden auspioniert)
- ❖ USB-Sticks  
(2006: Kollege von SNT „verliert“ USB-Sticks im Rahmen eines Security Audits)
- ❖ Gezielt zugesandte E-Mails  
(pdf.exe, Makroviren in Worddokumenten & Co.)
- ❖ Hack von Serversystemen
- ❖ Mitarbeiter installiert mutwillig Spyware auf Servern, Arbeitsrechnern oder PDAs

# Erkennungsraten bei Trojanern, Keyloggern und Rootkits



Spyware

# Massenmalware vs. Businessmalware

## *Massenmalware*

- ❖ Hauptmotivation: Botnetze (DDOS-Attacken, Spamming, distributed Hacking)
- ❖ Angriff gegen **Unbekannt**
- ❖ Muss sich gegen **alle** Antivirenlösungen behaupten
- ❖ Auf **maximale** Verbreitung ausgelegt

## *Businessmalware*

- ❖ Hauptmotivation: Spionage (Keylogger, Screenshots, Datentransfer)
- ❖ Das Opfer ist **bekannt**
- ❖ Muss nur **eine** Antivirenlösungen überwinden (auf Arbeitsrechnern)
- ❖ **Einmaliges** Sample (worst case)

# Massenmalware vs. Businessmalware

## *Massenmalware*

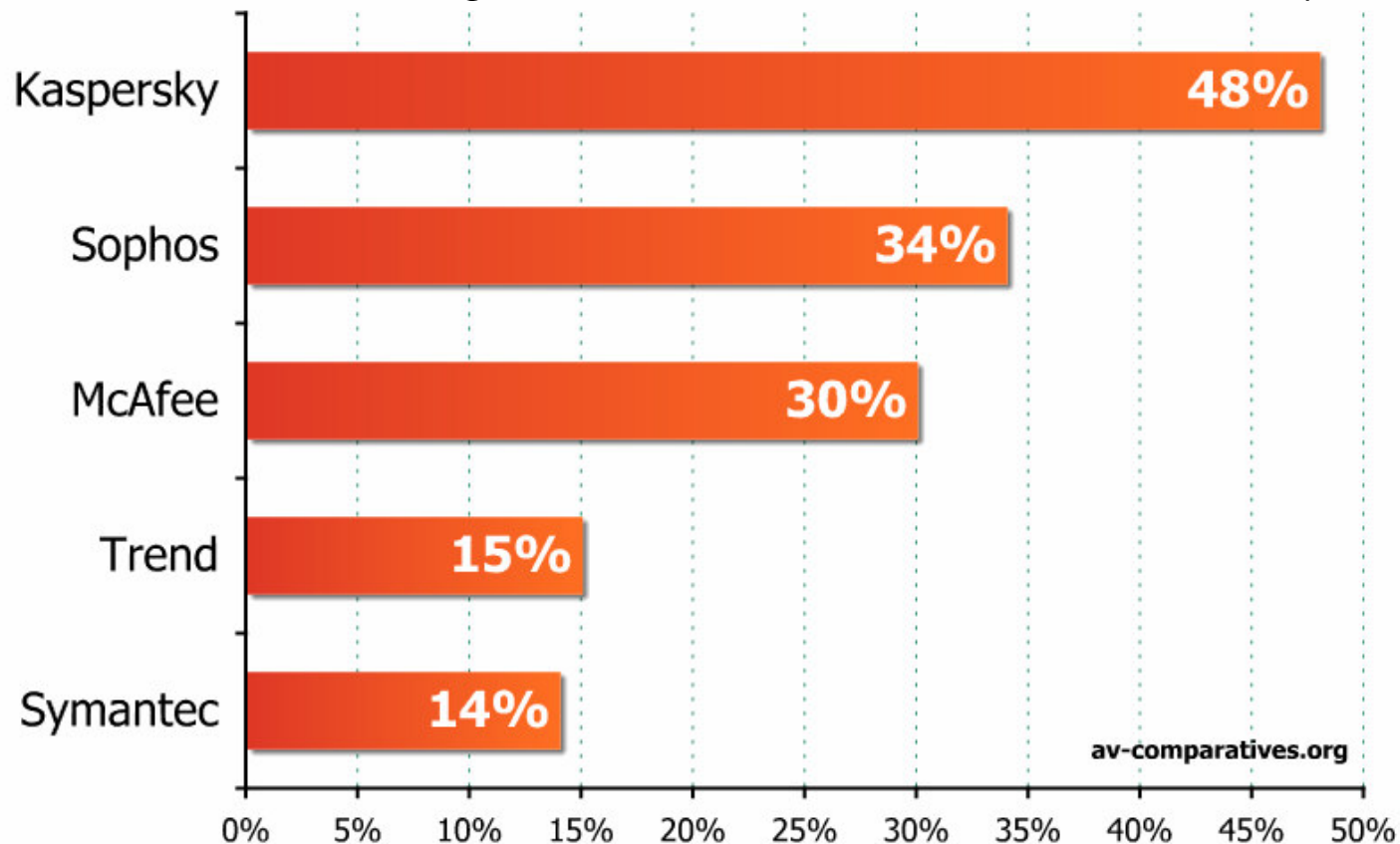
- ❖ Hauptmotivation: Botnetze (DDOS-Attacken, Spamming, distributed Hacking)
- ❖ Angriff gegen **Unbekannt**
- ❖ Muss sich gegen **alle** Antivirenlösungen behaupten
- ❖ Auf **maximale** Verbreitung ausgelegt

## *Businessmalware*

- ❖ Hauptmotivation: Spionage (Keylogger, Screenshots, Datentransfer)
- ❖ Das Opfer ist **bekannt**
- ❖ Muss nur **eine** Antivirenlösungen überwinden (auf Arbeitsrechnern)
- ❖ **Einmaliges Sample (worst case)**

## Schutz durch *proaktive* Technologien

*Erkennungsraten mit codebasierter Heuristik (KAV 5)*



# Schutz durch *proaktive* Technologien

## ***Zusätzlich: Zugriffskontrolle (unmittelbarer Schutz)***

- ❖ Unerlaubte Zugriffe auf andere Programme / Prozesse
- ❖ Änderungen der Registry
- ❖ Versenden von Daten über das Netzwerk

## ***Zusätzlich: Verhaltensbasierte Heuristik (fortlaufend)***

- ❖ Scoringsystem - Aktivitäten werden im Hintergrund protokolliert
- ❖ Wird ein Schwellenwert überschritten, erfolgt die Einstufung als Malware

# Schutz durch *proaktive* Technologien

## *Ergebnis*

- ❖ Durch Kombination aller proaktiven Techniken erreichte die neue Kaspersky Internet Security 6.0 im Test von av-comparatives (Juni 2006) eine Erkennungsrate von über 90 Prozent
- ❖ Problem: Anpassung von Malware an die vom Unternehmen verwendete AV-Lösung
- ❖ Lösung: Regelmäßige Updates der Heuristik durch Signaturupdates

## Reaktion nach Malwarefund

- ❖ Schicken Sie verdächtige Dateien zur Überprüfung an uns
- ❖ Ruhe bewahren – der Angreifer sollte nicht wissen, dass er entdeckt wurde
- ❖ Das betroffene System vorerst nicht verwenden, aber auch nicht ausschalten
- ❖ Umgehend forensische Untersuchung durch Fachkräfte einleiten



## Präventivmassnahmen

- ❖ Security Awareness schaffen bei Administratoren und Anwendern
- ❖ Realistische Security Policy
- ❖ Regelmässige Signaturupdates – nicht nur Malwaresignaturen, sondern auch Updates der Heuristik erfolgen auf diesem Weg.
- ❖ Nicht nur auf eine Lösung verlassen – zu AV-Lösungen serverseitig noch Intrusion Detection Systeme installieren
- ❖ Notfallplan für den Fall eines Angriffs vorbereiten, und regelmässig aktualisieren

# Vielen Dank

*Ihre Fragen, bitte!*