Ældre Sagen er alles sag

Malware & Anti-Virus
IT Temamøde Distrikt 9

Finn Larsen, Ældre Sagen Rudersdal
mail: fil@mail.dk

Ældre Sagen

Hvad er malware ?

- Ifølge Wikipedia: Ondsindet programkode, der gør skadelige eller uønskede ting på de computere, de kører på.
- Virus (f.eks trojansk hest eller orm) giver kontrol over PC til en ondsindet server
- Spyware stjæler personfølsomme oplysninger
- Adware viser uønsket reklameflimmer
- Ransomware tager Windows som gidsel for at kræve løsesum
- **P**otentially **U**nwanted **P**rograms installeres uden brugerens ønske
- Hoax (fup virus) skræmmer eller narrer folk
- Uønskede toolbars, f.eks ASK og AVG som stjæler søgemaskinen

Hvad beskytter mod malware ?

- Ugentlig image backup af harddisk. Men det gør folk jo ikke !
- Straks-installation af alle opdateringer til Windows, Java, Adobe Flash og Reader ...
- Firewall stopper uønsket ind- og udgående nettrafik
- Antivirus program stopper de fleste vira
- 100% beskyttelse umulig
- Mange nye vira hver dag, gamle vira muterer

Hvordan beskytter man sig ?

- Opdateringer kan automatiseres med *Heimdal, Secunia* eller *avast!*
- *Windows Firewall* er helt OK
- Godt antivirus program

ÆldreSagen

Hvilke antivirus er pt. bedst ?

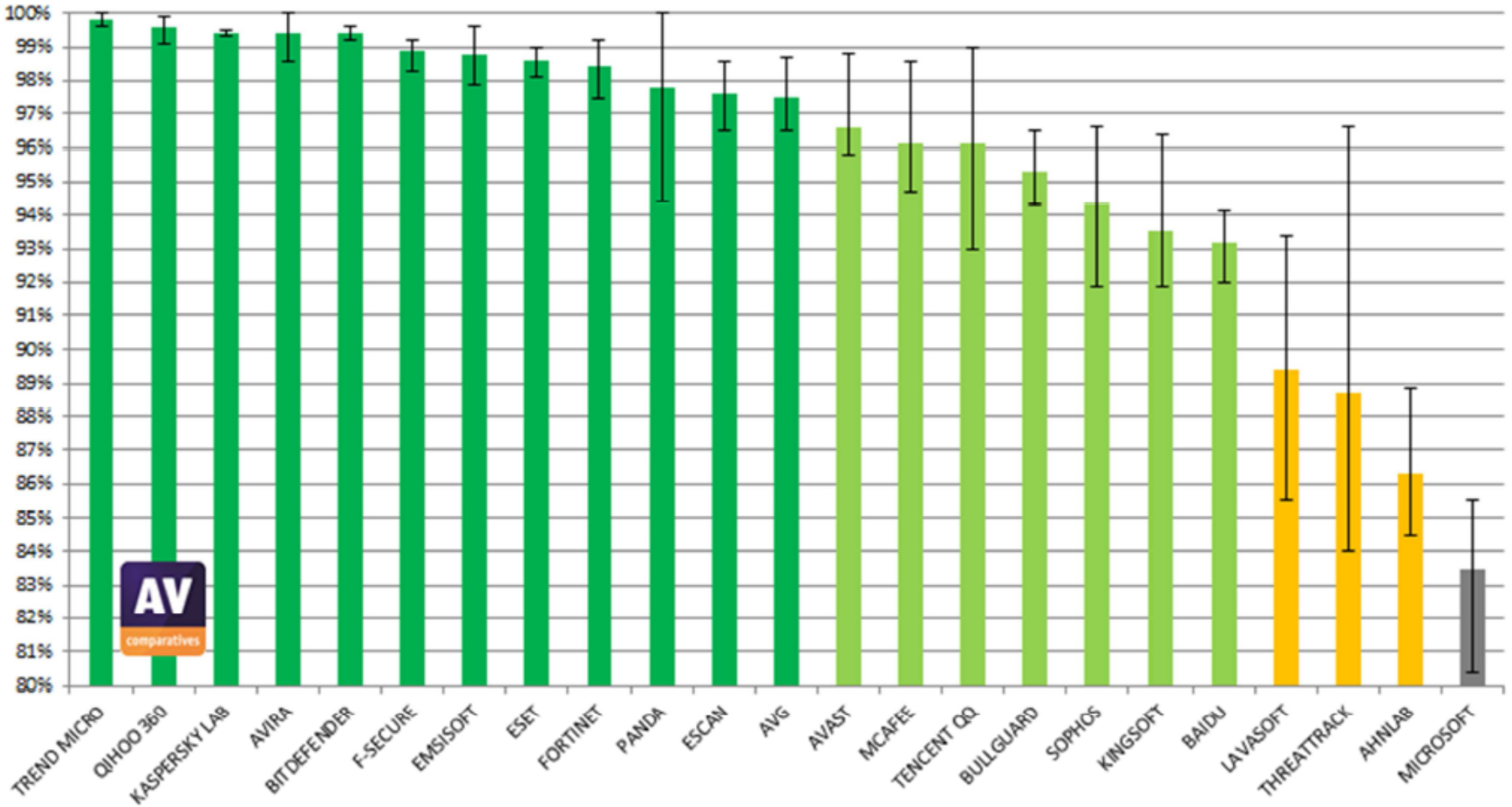
- *Bitdefender Antivirus Plus*
- *Kaspersky Anti-Virus*
- *Avira Antivirus Pro*
- *Trend Micro Antivirus + Security*
- *ESET NOD32 Antivirus*

Hvorfra ved vi det:
www.av-comparatives.org og http://www.av-test.org/en/

Reference materiale - eksempel

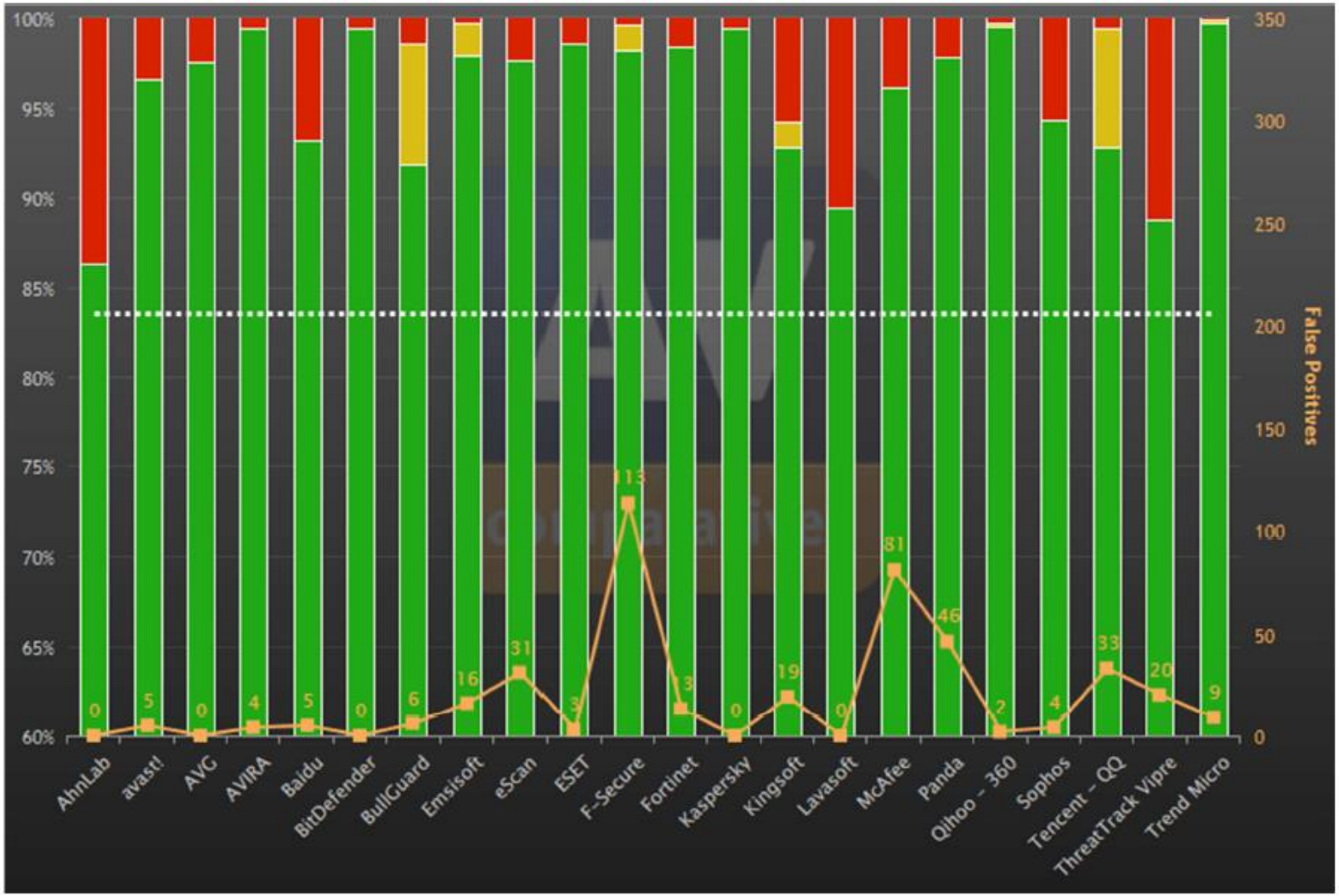
Whole Product Dynamic "Real-World" Protection Test – (August-November 2014)

www.av-comparatives.org



Ældre Sagen

Reference materiale - eksempel



Ældre Sagen

Hvilke gratis antivirus er bedst ?

- *avast! Free Antivirus*
- *AVG AntiVirus Free*
- *Avira Free Antivirus* (kun engelsk)
- *Bitdefender Antivirus Free Edition* (kun engelsk)

Ældre Sagen

Betalt antivirus er bedre end gratis

- *Windows Defender* stopper (by design) kun ca. 80% af kendt malware
- Opdatering og skanning med *Windows Defender* er meget ressourcekrævende.
- Gratis versioner har reduceret funktionalitet ift. betalingsversioner
- Gratis versioner presser / narrer til installation af prøveversion af betalt antivirus
- AVG og avast! kan efter første år kun forlænges med stort besvær
- AVG lokker til installation af *AVG Toolbar*, som udskifter søgemaskinen

Hvad gør man ved en inficeret PC ?

- Først forsøges Systemgendannelse i Fejlsikker Tilstand til en dato før infektion
- Genskab harddisken fra image backup, hvis muligt
- Så skanning med Malwarebytes i Fejlsikker Tilstand
- Derefter skanning med installeret antivirus i Fejlsikker Tilstand hvis muligt
- Hvis det ikke får Windows op at køre, kan man få hjælp fra Linux ved skanning med hhv. *Bitdefender Rescue CD*, *Avira Rescue CD* og *avast! RedningsDisk* indtil ingen vira findes
- Hvis alt mislykkes, retableres Windows til fabriksindstillinger fra Recovery partitionen, andre programmer installeres og systemindstillinger tilpasses forfra