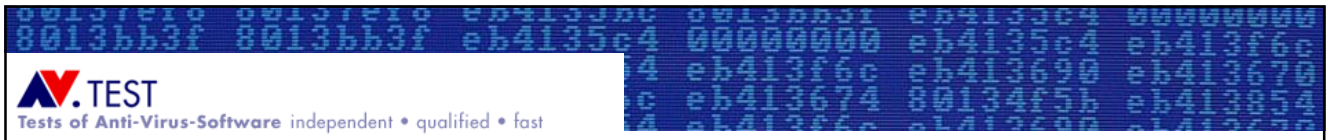


Useful and useless statistics about viruses and anti-virus programs

Dipl.-Ing. Maik Morgenstern and Hendrik Pilz
AV-Test GmbH, Magdeburg, Germany

Presented at CARO 2010 Helsinki

http://www.av-test.org

AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

Agenda

- Disclaimer
- The average anti-malware product
- The average malware
- The typical day in anti-malware industry
- Serious and not so serious implications
- Conclusions
- Q&A

AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

Disclaimer

- Not necessarily a scientific presentation
- Bases on data from AV-Test only
- May not be representative
- We are just talking about numbers
- We are not claiming anything and we could be wrong with what we say
- Still, some numbers could make you think

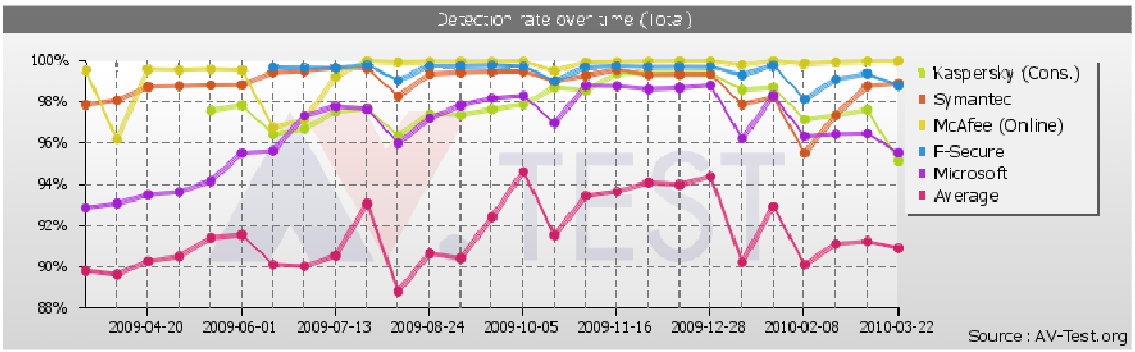
AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The average anti-malware product

- Based on data from about 30 products (2010)
  - Installer Size: 69,6 MB
  - Size on Disk: 265,5 MB
  - Number of Signatures: 3.666.872
  - Size of Signatures: 84,4 MB
  - Price: 32 €
  - Updates per Day: 6
  - WildList Detection: (virtually) 100%
  - Zoo Detection: 91,59%
  - False Positives: 0,00157%

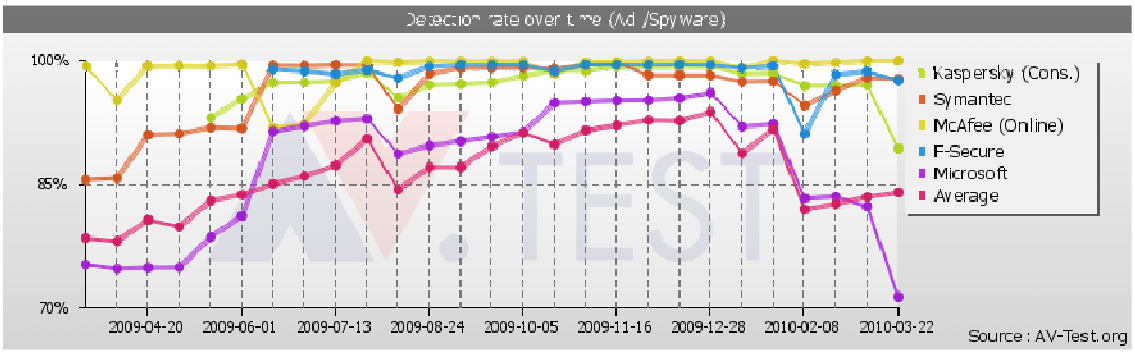
AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The average anti-malware product



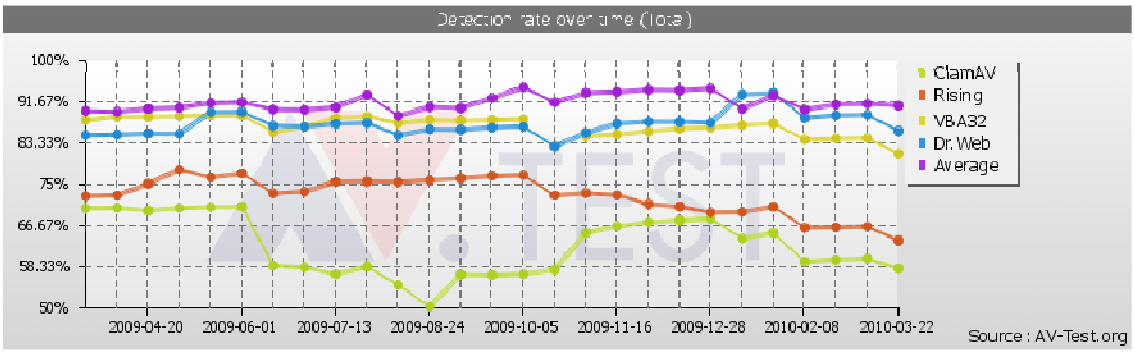
AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The average anti-malware product



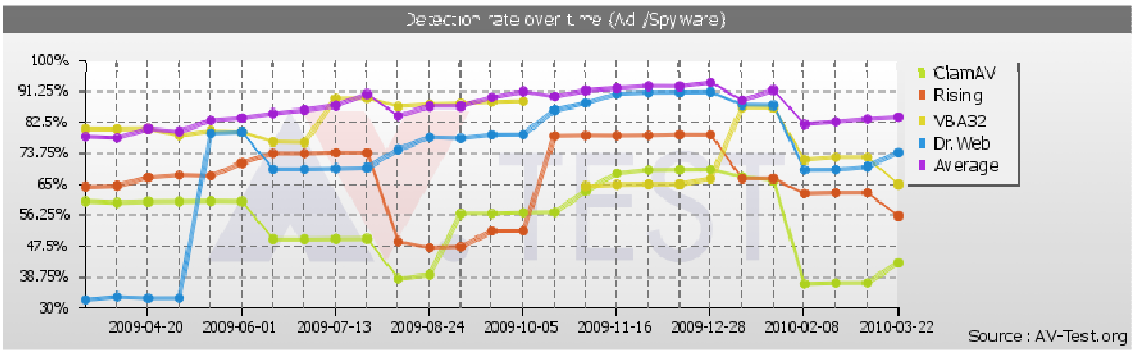
AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The average anti-malware product



AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The average anti-malware product



AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The average anti-malware product

- Based on data from about 20 products (2005)
  - Installer Size: 12,6 MB
  - Size on Disk: 87,9 MB
  - Number of Signatures: 104.509
  - Size of Signatures: 7,7 MB
  - Price: 45 €
  - Updates per Day: 2
  - WildList Detection: (virtually) 100%
  - Zoo Detection: 96,04%
  - False Positives: 0,03%

AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The average anti-malware product

- Comparison
  - TBD

AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The average malware

- In the year 2010
  - About 486,87 KB in size
  - Most likely a PE File
    - If not, then maybe HTML/PHP/JavaScript, PDF, some Image or Flash …
  - Probably a Trojan (52%), maybe a Worm (11%), a Backdoor (8%), Downloader (8%) or a Rogue application (6%)
  - Packed, probably by a custom packer (35%)
    - If not, then most likely UPX (29%), AsPack (11%), NullSoft (5%), PE Compact (3%), Themida (2%)
  - Detected under 6-7 different names
  - Usually detected after 2-4 hours

AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The average malware

- In the year 2005
  - About 180,01 KB in size
  - Most likely a PE File
    - If not, then maybe HTML/PHP/JavaScript, Batch File or Script
  - Probably a Trojan (35%) or a Backdoor (28%), maybe a Virus (18%) or a Worm (14%)
  - Packed, probably by one of the famous packers:
    - UPX (31%), FSG (14%), PE Compact (10%), Morphine (6%), AsPack (5%), NsPack (4%), uPack (4%)
  - Detected as the same family by all products
  - Usually detected after 10-12 hours

AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The average malware

- Comparison
  - TBD

AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The typical day in anti-malware industry

- In 2010
  - 574 Signature- and Program-Updates released per day
    - Thats over 17.000 per month and over 200.000 in a year
  - 17 GB of Updates downloaded by AV-Test per day
    - Thats over 510 GB per month and over 6120 GB in a year
  - Over 50.000 new unique samples received
    - Thats over 1.500.000 per month and nearly 20.000.000 in a year

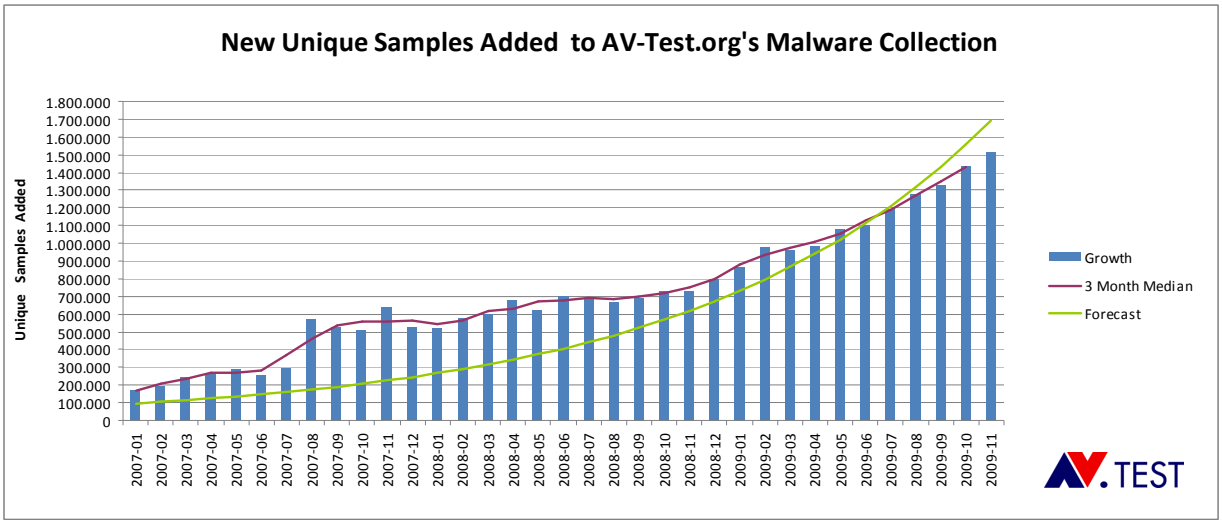
AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The typical day in anti-malware industry

- In 2005
  - 114 Signature- and Program-Updates released per day
    - Thats over 3.400 per month and over 40.000 in a year
  - 1,2 GB of Updates downloaded by AV-Test per day
    - Thats 36 GB per month and about 400 GB in a year
  - Over 360 new unique samples received
    - Thats over 10.000 per month and nearly 130.000 in a year

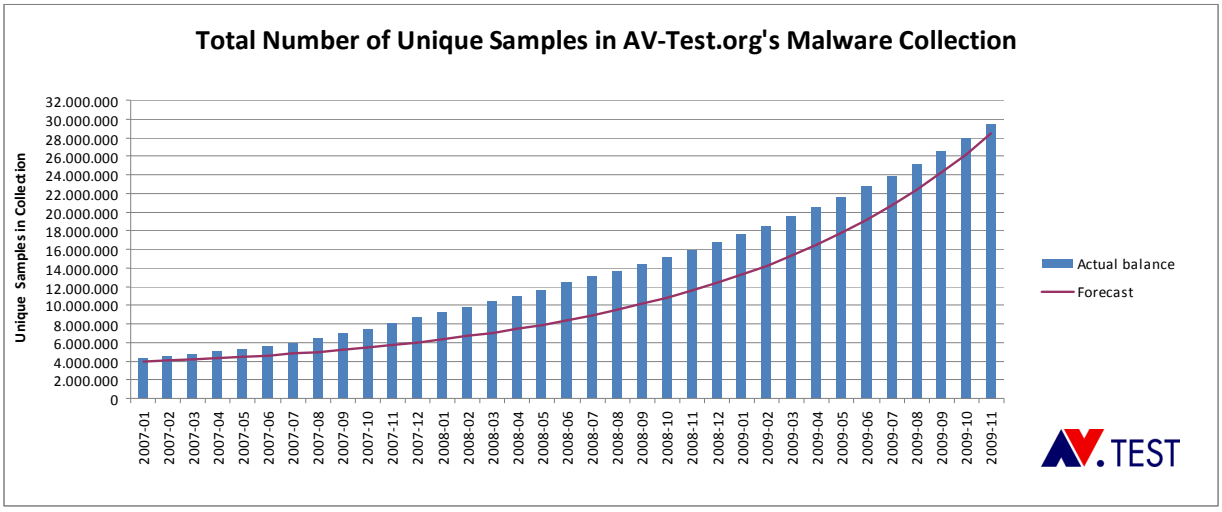
AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The typical day in anti-malware industry



AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The typical day in anti-malware industry



AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The typical day in anti-malware industry

- Comparison
  - TBD

AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

Serious and not so serious implications

- TBD

AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

Conclusions

- There are a lot of numbers and statistics to measure and to come up with
- Not all of them are useful
  - No product is like the average
- Those that are useful may only be useful in a limited time frame
  - Detection rates change, depending on sample set, signature database, …
- Some developments and growth rates can be estimated, many can't
  - It is nothing more than an estimation

AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

Q&A

Thank you very much for your attention!

Questions?